# FRAME RELAY ACCESS UNIT MODEL 9620/9621

## TECHNICAL REFERENCE

**Document No. 9621-A2-GH30-00**

August 1997

PARADYNE™

## Notice



## Warranty, Sales, and Service Information

Contact your sales or service representative directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, or training, use one of the following methods:

- **Via the Internet:** Visit the Paradyne World Wide Web site at http://www.paradyne.com
- **Via Telephone:** Call our automated call system to receive current information via fax or to speak with a company representative.
  - — Within the U.S.A., call 1-800-870-2221
  - — International, call 813-530-2340

## Trademarks

## EMI Warnings

### ⚠ WARNING:

**This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.**

**The authority to operate this equipment is conditioned by the requirements that no modifications will be made to the equipment unless the changes or modifications are expressly approved by Paradyne.**

### ⚠ WARNING:

**To Users of Digital Apparatus in Canada:**

**This Class A digital apparatus meets all requirements of the Canadian interference-causing equipment regulations.**

**Cet appareil numérique de la classe A respecte toutes les exigences du règlement sur le matériel brouilleur du Canada.**

## Important Safety Instructions

1. Read and follow all warning notices and instructions marked on the product or included in the manual.
2. The power supply for this product is intended to be used with a 3-wire grounding type plug – a plug which has a grounding pin. This is a safety feature. Equipment grounding is vital to ensure safe operation. Do not defeat the purpose of the grounding type plug by modifying the plug or using an adapter.

   Prior to installation, use an outlet tester or a voltmeter to check the ac receptacle for the presence of earth ground. If the receptacle is not properly grounded, the installation must not continue until a qualified electrician has corrected the problem.

   If a 3-wire grounding type power source is not available, consult a qualified electrician to determine another method of grounding the equipment.
3. Slots and openings in the cabinet are provided for ventilation. To ensure reliable operation of the product and to protect it from overheating, these slots and openings must not be blocked or covered.
4. Do not allow anything to rest on the power cord and do not locate the product where persons will walk on the power cord.
5. Do not attempt to service this product yourself, as opening or removing covers may expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.
6. General purpose cables are provided with this product. Special cables, which may be required by the regulatory inspection authority for the installation site, are the responsibility of the customer.
7. When installed in the final configuration, the product must comply with the applicable Safety Standards and regulatory requirements of the country in which it is installed. If necessary, consult with the appropriate regulatory agencies and inspection authorities to ensure compliance.
8. A rare phenomenon can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate buildings are **interconnected**, the voltage potential may cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action prior to interconnecting the products.
9. This product contains a coin cell lithium battery that is only to be replaced at the factory. **Caution:** There is a danger of explosion if the battery is incorrectly replaced. Replace only with the same type. Dispose of used batteries according to battery manufacturer's instructions. **Attention:** Il y a danger d'explosion s'il y a remplacement incorrect de la batterie. Remplacer uniquement avec une batterie du meme type. Mettre au rebut les batteries usagees conformement aux instructions du fabricant.
10. In addition, if the equipment is to be used with telecommunications circuits, take the following precautions:
    - — Never install telephone wiring during a lightning storm.
    - — Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
    - — Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
    - — Use caution when installing or modifying telephone lines.
    - — Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
    - — Do not use the telephone to report a gas leak in the vicinity of the leak.

# Contents

## 2 Management Control and IP Addressing



## 3 Typical Applications



## 4 Setting Up

# 5 Troubleshooting and Maintenance

# A Menu Hierarchy



# B Configuration Worksheets

# C MIB Descriptions

# About This Manual

## Purpose and Intended Audience

This reference contains information needed to properly set up, configure, and verify operation of the FrameSaver 9620 access unit. It is intended for system designers, engineers, administrators, and operators.

You must be familiar with the functional operation of digital data communications equipment and frame relay networks.

## Document Organization

| Section | Description |
|---|---|
| Chapter 1 | *About the FrameSaver 9620.* Describes the access unit and its features, and supported SNMP MIBs. |
| Chapter 2 | *Management Control and IP Addressing.* Describes how you establish a management link and configure end-to-end management control. Also provides guidelines for selecting an IP addressing scheme and shows examples of typical schemes with subnet masks assigned. |
| Chapter 3 | *Typical Applications.* Shows typical applications of the access unit in a frame relay network. |
| Chapter 4 | *Setting Up.* Provides instructions for configuring the access unit. Also includes a recommended order for setup, how to enter identity information, how to set date and time, and backup procedures. |
| Chapter 5 | *Troubleshooting and Maintenance.* Provides troubleshooting and test procedures, dial-out procedures, how to maintain directories and ISDN call profiles, and how to reset or clear performance statistics, and how to reset the access unit. Also describes local and remote management of the access unit. |

| Section | Description |
|---|---|
| Chapter 6 | *Security and Logins.* Describes how to administer security, as well as instructions for logging in or out once security has been set up. Backup security is also discussed. |
| Appendix A | *Menu Hierarchy.* Contains a graphical representation of how the user interface screens are organized. |
| Appendix B | *Configuration Worksheets.* Provides worksheets for recording configuration option settings. |
| Appendix C | *MIB Descriptions.* Provides clarification for the MIB objects when it is not clear how the object definition in the RFC is related to the access unit. |
| Appendix D | *Standards Compliance for SNMP Traps.* Describes the access unit's compliance with SNMP format standards and with its special operational trap features. |
| Appendix E | *Cables, Connectors, and Pin Assignments.* Identifies cables used with the access unit and provides pin assignments for them, along with those of the connectors/interfaces. |
| Appendix F | *Technical Specifications.* |
| Appendix G | *Equipment List.* Lists related equipment. |
| Glossary | Defines acronyms and terms used in this guide. |
| Index | Lists key terms, acronyms, concepts, and sections in alphabetical order. |

# Conventions Used

| Convention Used | When Used |
|---|---|
| *Italic* | To indicate variable information (e.g., Port-*n*, indicating Port 1 or 2). |
| *Menu selection sequence:* | To provide an abbreviated method for indicating the selections to be made from a menu or selections from within a menu before performing a procedural step (e.g., *Main Menu→Status→System and Test Status*). |
| (Path:) | To provide a check point that coincides with the menu path shown at the top of the screen. Always shown within parentheses so you can verify that you are referencing the correct table (e.g., Path: main/config/alarm). |
| Brackets [ ] | To indicate multiple selection choices when multiple options can be displayed (e.g., Clear [*Network/Port-1/Port-2/BRI-B1*] Statistics). |

# Related Documents

| Document Number | Document Title | Purpose/Focus |
|---|---|---|
| 9621-A2-GB20 | FrameSaver 9620 User's Guide | Provides feature, user interface, log in and out, session start and stop information, as well as how to display information. Includes status, statistics, and LEDs information, as well as alarms and messages.<br>Includes a *Quick Reference* for easy navigation through menus and a summary of the configuration options. |
| 9621-A2-GN10 | FrameSaver 9620 Network Access Module (NAM) Installation Instructions | Describes how to install a NAM in a 1-slot housing. Includes cabling, operation verification, technical specifications, and pin assignments. |
| 9000-A2-GN10 | 1-Slot Assembled Access Unit, Installation Instructions | Describes how to install a fully assembled 1-slot access unit. Includes technical specifications. |
| 9000-A2-GN11 | 1-Slot Access Unit, Wall Mounting Kit, Installation Instructions | Describes how to install the mounting hardware with an access unit so the 1-slot assembled unit can be mounted onto the wall. Includes technical specifications. |
| 9000-A2-GN13 | Power Cord/Transformer Installation Instructions | Describes how to install the power cord and transformer for a 1-slot unit. Includes technical specifications. |
| 9000-A2-GN21 | Universal Power Supply Installation Instructions | Describes how to install the universal power supply/transformer and the power cord for a 1-slot unit used outside the United States and Canada. Includes technical specifications. |
| 9000-A2-GN19 | ISDN BRI Dial Backup Module (DBM) Installation Instructions | Describes how to install a DBM on a NAM. Includes cabling, operation verification, technical specifications, and pin assignments. |
| 9621-A2-GX40 | FrameSaver 962x, Safety and Regulatory, Warranty and Service Information | Provides safety and regulatory, and warranty and service information. |

# About the FrameSaver 9620

# 1

## Overview

The FrameSaver 9620 access unit provides an interface between the customer premises equipment (CPE) and a frame relay network to the public frame relay network facilities.

It provides a variety of features and capabilities which support:

- Aggregated packet applications
- Data compression
- Diagnostic functions
- Management connectivity
- Automatic DLCI configuration and cross-connection
- Automatic backup and restoration (optional feature)

# What Is Needed to Use Access Units in My Network?

The following components are available when including access units in your network:

| Component | Function |
|---|---|
| FrameSaver 9620 Network Applications Module (NAM) | Interface between the frame relay network and the customer premises equipment (CPE). |
| Dial Backup Module (DBM) | An option that can be ordered to provide backup internally, so you do not need an external modem. |
| 1-Slot Standalone Housing | Accommodates 1 NAM or NAM/DBM. Comes with a 120 Vac power supply and cord. Used primarily at remote sites. |
| 120 Vac Power Supply | Provides AC power for the housing. |
| 1-Slot Access Unit Wall Mounting Kit | Permits the 1-slot housing to be mounted on a wall. |

# Features

The FrameSaver 9620 offers the following features:

- **Frame Relay Aggregation.** Provides the ability to multiplex frames coming from multiple frame relay devices onto a single network connection or PVC.
  - — Provides aggregation of up to three frame relay interfaces when an ISDN BRI DBM is installed: two DTE ports and one backup interface.
  - — Provides data prioritization based on PVCs.
  - — Supports multiple PVCs on an interface.
  - — Provides monitoring and enforcement of CIRs on a per-PVC basis.
  - — Supports the LMIs – Annex-A, Annex-D, and Standard UNI (user network interface) management protocol.

- **Frame Relay Aware (FRAW).** Provides support for diagnostic and network management features over the frame relay network.
  - — Provides diagnostic capabilities, including PVC loopbacks and pattern tests.
  - — Supports in-band management channels over the frame relay network using dedicated PVCs.
  - — Multiplexes management channels with the bandwidth of specific data-carrying PVCs over the frame relay network using a proprietary mechanism.
  - — Allows a dedicated PVC over a DTE port for management of the local unit. This takes advantage of a router to provide management of remote units with which it is colocated.
  - — Does not require extra ports and cables to get management data into the access unit via the router.
- **Data Compression.** Supports compression of data on one DTE port.
  - — In Frame Relay mode, supports selective compression of up to six customer-configured DLCIs.
  - — In Bit-Synchronous mode, supports compression of HDLC-like protocols with frame relay encapsulation over a preconfigured PVC.
  - — Supports DTE port rate of up to 256 kbps with continuous clock rate flow control.
  - — Supports short packet by-pass mode. Short packets will not be compressed and will be transmitted to the network using transparent mode.
  - — Maximizes throughput by invoking a reliable protocol only when packet loss is sensed.
- **Configuration Shortcuts.** Provides simplified setup configuration, and automatic DLCI configuration and cross-connection.
  - — *Configuration Templates.* Provides templates that simplify setup of the access unit based upon how the unit will be used in the network.
  - — *Frame Relay Discovery Methods.* Provides automatic configuration of DLCIs and connection to network DLCIs.

- **Integral ISDN (Integrated Services Digital Network) Backup.** If the ISDN BRI DBM option is installed, provides automatic backup of data via an alternate route when network or access line failures occur.
  - Provides periodic testing of the circuit to assure that the switched network is available.
  - Supports automatic initiation of a backup call when there is a failure and establishment of an alternate data path so manual intervention is not needed.
  - Supports automatic restoration of data when service returns to normal.
  - Supports alarm generation and an LED warning when the network goes down.
  - Provides call security that restricts unauthorized access to the unit.
- **SNMP (Simple Network Management Protocol) Management.** Provides network management via an external SNMP management system using industry-standard and product-specific MIB (Management Information Base) objects.
- **NMS (Network Management System) Support.** Supports the following SNMP-managed system applications:
  - HP OpenView for Windows
  - HP OpenView for Unix
  - IBM's NetView AIX
- **Local Management.** Provides local management through:
  - COM port for async terminal or NMS connection
  - PVC connection configured for the DTE port (Port-1 or Port-2)
- **Remote Management.** Provides remote management:
  - Out-of-band, using an external modem or an ISDN BRI DBM
  - In-band, using the frame relay network
  - Via Telnet
- **Data Port Rates.** Supports 4.8, 9.6, 14.4, 16.8, 19.2, 24, 28.8, 38.4, 48, 56, and 64 kbps. With very bursty traffic, where you want to reduce latency, or when Port 1 has compression enabled, supports additional rates of 128, 192, and 256 kbps.
- **DDS (Digital Data Service) Rates.** Operates at 56 and 64 kbps (clear channel).

- **Multiple Management Paths.** Provides multiple communication methods for sending/receiving management data:
  - — Between the network management system and FrameSaver 9620
  - — Between the FrameSaver 9620 and a router or internet device through the communications (COM) port
  - — Using in-band management on either the network or DTE port

    A proprietary method using multiplexed DLCIs, called EDLCIs, provides a way of multiplexing management data with customer data so that no additional PVCs are required.
- **IP (Internet Protocol) Connectivity.** Supports connectivity within an IP network for up to 300 IP host and/or network routes and provides IP routing for SNMP, Telnet, and file transfer protocol (FTP) message connectivity without requiring direct connections.
- **Alarm and Fault Condition Indication.** Provides the capability to attach a terminal or printer to display or print alarm messages.

  Alarms or traps generated include: crossed-pair connection, no signal, out of service, out of frame, excessive bipolar violations, logical link or DLCI is down/up, frame relay DLCI is down/up, compression connection is down, low compression ratio, and DBM and ISDN network failure.
- **Extensive Testing Capability.** Provides a variety of tests to diagnose device, network, and PVC problems. Diagnostic tests that can be selected include:
  - — *Physical Tests* for an interface: Network, Port-1, or Port-2.
  - — *PVC Tests* for an interface: Network, Port-1, Port-2, or BRI-B1.
  - — *Loopbacks* for an interface include: network CSU and DSU, external DTE-initiated, PVC, and PVC connectivity loopbacks.
  - — *Pattern Tests* for an interface include: 511 and 55 hexadecimal test patterns.
  - — Self-test
  - — Lamp test
- **SNMP MIB (Management Information Base) Object Test Commands.** Supports the same testing capability as the user interface.

- **Extensive Monitoring Capability.** Provides status information to help you keep track of and evaluate the unit's and network's operation via:
  - *Status Branch/Menu*. Provides system and test status, LMI (local management interface)-reported DLCI statuses on each interface, source and destination PVC (permanent virtual circuit) connection statuses for each interface, and DBM interface status information.
  - *Performance Statistics*. Provides physical and frame relay statistics for each interface, and PVC and compression statistics for each DLCI.
  - *Faceplate LEDs*. Provides unit and interface monitoring that includes network and synchronous data port statuses, as well as backup status if an ISDN BRI DBM is installed.

    An additional feature allows you to select which DTE port is being monitored via the faceplate LEDs, as well as allowing you to monitor all LEDs via the user interface.
- **Extensive Statistics Gathering.** Provides a complete view of the network's, each data port's, and the DBM's (if installed and enabled) performance through the statistical data collected from those interfaces to assist in determining the duration of a condition or event.
  - Quick and easy access to seven sets of statistics is provided, selectable from a menu.
  - You can select a set of statistics for each interface's physical performance; frame relay link, error, and LMI performance; as well as PVC and compression performance.
  - *Physical DDS network performance statistics* collected count occurrences of the following: no signal, out of service, out of frame, BPVs, and excessive BPVs.
  - *Physical DTE port performance statistics* collected count the following: over and underruns, CTS and DTR lost events, CRC errors, and non-octet frames.
  - *Physical DBM performance statistics* collected, if an ISDN BRI DBM is installed, count occurrences of the following: calls attempted, originated, answered, and rejected, as well as average duration.
  - *Frame relay link, error, and LMI performance statistics* collected count the following: frames and characters sent and received, and FECNSs and BECNSs received; invalid frames, short and long frames, invalid and unknown DLCIs, and unknown errors; and status messages, reliability and protocol errors, and inactives.

- — *PVC performance statistics* collected count the following: Tx and Rx characters, Tx and Rx frames, frames and frames dropped, frames within and exceeding CIR, frames with DE bit set, BECN and FECN frames.
- — *Compression performance statistics* collected for selected DLCIs count errored frames received on the network interface and history resets.
- — All but the DBM counters go up to 4,294,967,294, with a + indicator when that number is exceeded; the DBM counters go to 999,999.

- **Menu-Driven User Interface.** Provides an easy to use, menu-driven interface to configure, manage, and maintain the access unit, and access the extensive diagnostic capability locally or remotely. The user interface is accessed using an async (or other VT100-compatible) terminal, PC terminal emulation, or Telnet session.
- **Interoperability with T1 Frame Relay Access Units.** Operates with the frame relay aware (FRAW) capability of a Model 9120 access unit.
- **Two Software-Configurable Ports.** Provides configurability of ports for connection to either an EIA-232 or V.35 DTE device.
- **Two Customer-Specified Configuration Storage Areas.** Allows quick switching of the access unit's configuration.
- **Configuration Upload/Download and Software Download Capability.** Provides quick, cost-effective software upgrades, and quick transfer of configuration options to and from nodes using a standard file transfer protocol (FTP).
- **Security.** Provides multiple levels of security, which prevents unauthorized access to the unit.

  Security can be controlled by:

  - — Disabling any form of access to the unit.
  - — Requiring logins (login ID/password/access level combinations), with three access levels to select from: read-only, limited-access, and full-access.
  - — Enabling SNMP management, and specifying a community name and access level Read or Read/Write.
  - — Enabling SNMP management, and specifying the IP addresses of only selected NMSs.
  - — If the ISDN BRI DBM option is installed, specifying calling identifiers, screening all incoming calls, and only accepting calls from devices using one of the specified calling identifiers.

# SNMP Management Capabilities

The FrameSaver 9620 supports SNMP Version 1, and has the capability of being managed by any industry-standard SNMP manager using SNMP protocol.

## MIB Support

The following MIBs are supported:

- **MIB II (RFC 1213 and RFC 1573)** – Defines the general objects for use with a network management protocol in TCP/IP internets and provides general information about the FrameSaver 9620. MIB II is backward-compatible with MIB I.
- **Frame Relay DTEs MIB (RFC 1315)** – Defines objects for supporting both the network and synchronous data ports when the interface is configured to support the User side of the frame relay UNI.
- **RS-232-Like MIB (RFC 1659)** – Defines objects for managing RS-232-type interfaces (e.g., V.35, RS-422, RS-423, etc.) and supports synchronous data ports and management communication ports on the access unit.
- **Frame Relay Service MIB (RFC 1604)** – Defines objects for supporting both the network and synchronous data ports when the interface is configured to support the Network side of the frame relay UNI.
- **Enterprise MIB** – Supports execution of PVC tests and the display of DLCI connections within the access unit, as well as the devConfigAreaCopy group in the common area of this MIB, which allows the entire contents of one configuration area to be copied into another configuration area.

## COM Port-Supported Link-Layer Protocols

The access unit supports two link-layer protocols for connection to an external SNMP manager or network device via the COM port:

- Point-to-Point Protocol (PPP)
- Serial Line Internet Protocol (SLIP)

# About Congestion Control

As with any frame relay product, network congestion can cause problems. As long as there is little or no congestion in the network, data is transferred at high speeds with little or no delay or errors.

The following indicates how the access unit can be configured to handle congestion control:

- On the network side, the access unit can be configured to monitor its own traffic and enforce the CIR.*****
- On the user side, the access unit can be configured to monitor its own traffic and enforce the CIR.

CIR and Excess Burst Size are set for each DLCI on the PVC connection. Based upon the network-committed information rate and burst size, the access unit's inbound or outbound CIR enforcement can be set to mark a frame for discard eligibility, and forward or drop a frame. Contact your network supplier for the CIR and Excess Burst Size they will provide.

Setting a port's Inbound CIR Enforcement Mode (frames received from the frame relay interface) and Outbound CIR Enforcement Mode (frames sent over the frame relay interface) enforces CIR and Excess Burst Size.

**NOTE:**

If data compression is used and it is expected that the FrameSaver 9620's actual port throughput CIR will exceed the PVC's CIR, and the excess burst size will be exceeded, then do not select Standard or Discard as a CIR enforcement mode.

* CIR enforcement is also known as *traffic shaping*.

The following tables indicate how the access unit responds based upon the frame and the CIR enforcement setting. See the Inbound CIR Enforcement Mode, Outbound CIR Enforcement Mode, CIR (bps), and Excess Burst Size (Bits) configuration options in Tables 4-5 and 4-6 of Chapter 4, *Setting Up*.

- **Inbound CIR Enforcement configuration option:**

| If Frame is . . . | And Inbound CIR Enforcement is set to . . . | Then . . . |
|---|---|---|
| ■ Within CIR and<br>■ Within CIR plus excess burst size and<br>■ Not discard eligible | Forced | Frame forwarded |
| | Standard | |
| | Discard | |
| ■ Within CIR and<br>■ Within CIR plus excess burst size and<br>■ Discard eligible | Forced | Frame forwarded with DE set |
| | Standard | |
| | Discard | |
| ■ Above CIR but<br>■ Within CIR plus excess burst size and<br>■ Not discard eligible | Forced | DE set, then Frame forwarded |
| | Standard | |
| | Discard | |
| ■ Above CIR but<br>■ Within CIR plus excess burst size and<br>■ Discard eligible | Forced | Frame forwarded with DE set |
| | Standard | |
| | Discard | |
| ■ Above CIR plus excess burst size and<br>■ Not discard eligible | Forced | DE set, then Frame forwarded |
| | Standard | |
| | Discard | Frame discarded |
| ■ Above CIR plus excess burst size and<br>■ Discard eligible | Forced | Frame forwarded with DE set |
| | Standard | Frame discarded |
| | Discard | |

- **Outbound CIR Enforcement configuration option:**

| If Frame is . . . | And Outbound CIR Enforcement is set to . . . | Then . . . |
|---|---|---|
| ■ Within CIR and<br>■ Within CIR plus excess burst size | Forced | Frame forwarded |
| | Standard | |
| | Buffered | |
| ■ Above CIR but<br>■ Within CIR plus excess burst size | Forced | Frame forwarded with DE set |
| | Standard | |
| | Buffered | |
| ■ Above CIR plus excess burst size | Forced | Frame forwarded |
| | Standard | Frame discarded |
| | Buffered | Frame held until CIR not exceeded |

# About Data Compression

Data compression, available on Port 1 only, is a feature that allows higher DTE port rates over the DDS network, reducing network bandwidth, as well as cost and time for transmissions without losing data. When enabled, port rates up to 256 kbps are supported.

This feature supports the Frame Relay *Forum's Data Compression Over Frame Relay Implementation Agreement, FRF.9.*

**NOTE:**

The local and remote FrameSaver 9620s maintain a connection between their compressors. If the connection cannot be established because of network problems, an alarm is generated.

See Chapter 3, *Typical Applications*, for additional information.

## Throughput

Throughput (i.e., bits per second) is the amount of data, or number of data units per units of time, that passes through the network.

Throughput is a result of:

- Network and port rates
- Network error rate, affecting packet loss and the need to retransmit
- Compression ratio, achievable for the data being transmitted
- Protocol overhead imposed by compression and frame relay
- Latency imposed between two FrameSaver 9620s and by the network

Consider these and the following information when the data compression feature is enabled.

- Generally speaking, flow control is necessary, especially when packet sizes are large and files are compressed. Flow control and compression are less effective when sending short packets.
- When flow control is not used (when the DTE cannot accept flow control), transmitter overruns are likely, reducing performance. Selecting Clock (rate control) as the flow control method minimizes latency and prevents transmitter overruns and underruns.
- The type of data being compressed determines throughput. The more structured the data, the more compressible; the more random, the less compressible.

**NOTE:**

It is recommended that data compression be enabled on only one device on the data stream (e.g., access unit's data compression enabled, server's data compression disabled).

## Protocol Modes

Data compression supports two protocol modes:

- **Frame Relay Mode** – Used for DTEs that support frame relay operation. Compresses data on as many as 6 PVCs on Port 1 and combines these with uncompressed PVCs. The compressed Port 1 data can be aggregated with uncompressed data from Port 2, and transmitted on the DDS facility over designated frame relay PVCs.
- **Bit Synchronous Mode** – Used for DTEs that support any other HDLC-based protocol. Assumes Port 1 is carrying non-frame relay HDLC-like data. This data is compressed and encapsulated onto a single PVC, and combined with uncompressed PVCs from Port 2.

See DTE Type configuration option description in Table 4-2 of Chapter 4 for additional information.

## Compression Ratios

Data compression permits data coming from Port 1 to be compressed at ratios of 2:1, or more, for greater data transmission throughput. Up to six PVCs can be compressed. Generally speaking, English text yields a ratio of about 2:1; less structured data, like binary files or source code, yields lower ratios.

Compression is enabled on a per-DLCI basis using the Port 1 DLCI Records screen. When a compression ratio threshold for the DLCI is set, an alarm will be generated when the ratio falls below the threshold that was set.

## Determining a Flow Control Method

Flow control is a method used to control the flow of data from the DTE to the access unit and vice versa. It is required to ensure maximum throughput as compression ratios vary according to the nature of the data.

Two flow control methods are supported:

- **Variable Clock Rate** – Varies the clock rate to match the current compression ratio. This is the recommended method and should be used when the DTE is compatible with clock rate control.
- **CTS Signaling** – Uses CTS to prevent the DTE from sending more data than can be handled by the access unit. Used only when the DTE is not compatible with clock rate control.

See the Port 1 Compression configurations in Chapter 4 for more information.

## Short Packets Bypass

A short packet is a packet that contains less than 80 bytes of data. The FrameSaver 9620 can be configured to bypass compression of short packets when they occur to minimize overhead and latency in polled protocol environments, and to improve performance in environments where short packets are predominant.

You may want to experiment with enabling and disabling this configuration option to determine which setting optimizes performance given your network's traffic patterns.

## Optimizing Operation

Performance can be further optimized using the Optimize Based On configuration option. Selecting:

- **Throughput** – Optimizes compression to increase throughput, the amount of data transferred.
- **Latency** – Optimizes compression to decrease latency, the time it takes to transfer data from its source to its destination.

# About Configuration Shortcuts

Configuration shortcuts have been provided to simplify configuration of the FrameSaver 9620 and its features. Two types of configuration aids have been provided:

- **Configuration Templates** – Used primarily during initial configuration, when setting up the access unit. Each template enables or disables port configuration options. Selecting a configuration template that indicates the DTE ports that will be used causes the appropriate ports and options to be enabled or disabled. Only enabled port configuration options appear for customization.
- **FR Discovery Method** – Used for automatic PVC configuration within the access unit when the network interface is configured as the user side of LMI (the usual configuration). For each DLCI coming from the network, the unit creates a port DLCI, then connects them automatically. A discovery method must be selected for network-to-port DLCIs to be connected.

These configuration aids can be used together, or they can be used independent of one another. Initially, this feature can be used to speed setup of the FrameSaver 9620. Then, by selecting a frame relay discovery method, configuration and cross-connection of DLCIs can be performed within the access unit on an automatic and continuing basis.

**NOTE:**

If using the frame relay automatic configuration feature (FR Discovery) and the service provider does not use Annex D protocol, it is recommended that the network interface's LMI Protocol be pre-configured along with the Node IP Address, Subnet Mask, and DS0 allocations before the deployment of remote access units.

Refer to *Using Configuration Shortcuts* in Chapter 4, *Setting Up*, for additional information.

## About Alarms

The access unit can be configured to:

- Send alarm messages to an ASCII terminal or printer attached to the access unit's COM port.
- Dial out using an external modem connected to the access unit's COM port to send alarm messages to a remote ASCII terminal or printer.

See Chapter 4, *Setting Up,* for assistance in configuring alarms and Chapter 5 of the User's Guide, *Maintenance and Troubleshooting,* for more information about alarms.

## About Backup

The access unit can provide backup using either an external backup device like a modem or an internal ISDN BRI DBM (dial backup module). Backup limits data loss when the physical circuit fails.

The main distinction between external and internal backup is:

- **External backup device** – The device can answer or originate backup calls one destination at a time. The external backup device must provide backup security.
- **Internal ISDN BRI DBM** – The DBM can originate or answer calls to or from another destination. The DBM takes advantage of ISDN services for network backup and calling number identification service (CNIS) to provide backup security, with ISDN assuring the integrity of calling party identifiers.

The backup feature also supports manual call control. Refer to *Manual Dial Backup* in Chapter 5 for manual calling procedures.

**NOTE:**

If upgrading a FrameSaver access unit with an ISDN BRI DBM, you need software revision 2.0 or greater. Contact your sales or service representative if you need to upgrade your software.

## Backup Philosophies

Backup in the access unit is based upon two basic concepts:

- **Concept of an alternate destination.** By defining an alternate (or backup) path for data, data can be switched to the alternate destination path when the primary destination connection fails. This concept allows an alternate circuit (or path) to be defined for each primary destination circuit.

  Configuring a backup link, DLCI, and possibly a multiplexed DLCI (EDLCI) specifies this circuit. The circuit can be on the same physical port as the primary destination circuit, or it can be on a different port.

- **Concept that automatic backup is better.** Using the automatic backup feature immediately puts the unit into backup as soon as a network, LMI, or PVC failure is detected. A failure of the physical link between the access unit and the network or an external device can also initiate backup. This feature allows the unit to switch data to the backup path without operator intervention or the delay of waiting for the LMI to time out.

  A failure of the physical connection that will cause automatic backup to occur includes the following conditions:

  — No signal (NS)

  — Out of service (OOS)

  — Out of frame (OOF)

  — Excessive bipolar violations (BPVs)

  A failure of the logical connection that will cause automatic backup to occur includes:

  — LMI failure – T1 timer has expired a specified number of times. LMI Heartbeat (T1) is configured to monitor LMI.

  — DLCI failure – Declared inactive by the frame relay network.

  Automatic backup also allows an NMS to provide time-of-day backup control since the FrameSaver 9620 does not have an internal time of day clock for switching between automatic and non-automatic backup cycles. Refer to *Restricting Auto Backup Based Upon the Time of Day* in Chapter 4 for the procedure.

Being a frame relay aware product, the access unit continually monitors the condition of the frame relay physical and logical links. As soon as a failure is detected, the access unit initiates a backup call (provided the automatic backup feature is enabled), establishes an alternate connection, and switches data to the established backup link. All reconfiguration occurs automatically within the unit, entirely transparent to the connected DTE.

When the primary circuit recovers, returning to normal service, the access unit automatically restores data to the primary circuit.

Refer to Chapter 3, *Typical Applications*, for additional information. Chapter 4, *Setting Up*, provides assistance in configuring the access unit for backup.

## Using an ISDN BRI DBM

Available as an optional feature, the ISDN BRI DBM supports a variety of backup schemes. The access unit itself supports various LMI types and provides switching capability. Combined with the ISDN BRI DBM's capabilities, better, faster, and easier backup can be achieved.

Order:

- 1B+D service from your LEC (local exchange carrier), which supports one circuit-switched B channel with one SPID (service profile identification) number and one local phone number.
- CNIS (calling network identification service) for both the originating and answering units, which provides calling number identification for data traffic on the B channel.

When installed and enabled, the ISDN BRI DBM:

- Uses a B channel for backup, creating an alternate data path that goes to a different destination. A B channel can be configured to support the user or network side of the LMI and different LMI types. It can also be configured as a source or a primary destination, not just an alternate (backup) path or destination.
- Supports up to 3 Alternate Destination Profiles, which must be specified if the B channel is used for the backup link.

  Although multiple call profiles are supported, once backup is in progress on a B channel, all data is transmitted to the same destination until backup is terminated on that B channel and another destination specified.
- Incorporates congestion avoidance and response capability that helps eliminates limited-bandwidth bottlenecks while the access unit is in backup.

Even though the ISDN BRI DBM is used primarily for backup, source and primary destination circuits can also be configured on a BRI. If LMI is enabled on a B channel (frame relay Link Status set to Enable) and the access unit is configured to originate ISDN calls, the unit dials to establish a connection immediately after power-up, just like any other interface with a source and primary destination configured.

If the B channel is used as a primary or alternate destination link, the originating unit uses the call profile specified in the PVC Connection or Management PVC Table for the failed primary connection. Should an entire primary destination link fail on the unit configured as the backup originator, the first alternate destination link listed on the PVC Connection Table is used as the alternate destination link.

The ISDN BRI DBM terminates backup when the primary destination DLCIs are active once again, ensuring that the primary destination link and LMI are enabled. When the LMI on the primary destination link declares each primary destination DLCI active, the unit switches the data path from the alternate destination DLCI back to the primary destination DLCI.

When all alternate destination DLCIs have been switched back, the backup link is disconnected. That is the B channel when the backup link is configured on the DBM, or dropping DSR when the backup link configured is a data port.

Refer to Chapter 4, *Setting Up*, for assistance in configuring this feature, and Chapter 5 of the User's Guide, *Maintenance and Troubleshooting,* for information about backup messages.

Contact your sales representative to order this feature.

## Using an External Modem or Other Backup Device

A crossover cable is required when connecting an external modem (or other backup device) to one of the access unit's DTE ports. When an external backup device is used, the access unit assumes that all alternate data paths are to the same destination, and that the backup device will handle security.

When using an external backup device, the external device must be configured to dial another modem upon detecting raised DTR (data terminal ready), and the access unit's data port (connected to the external backup device) must be configured as the backup link (the alternate destination link) and to support the DTR control lead.

If the backup device is configured to originate backup, the access unit raises DSR (data set ready) when a failure is detected, signaling the backup device to dial another backup device. Once connection between the backup devices is established, data is switched to the alternate (backup) path.

A backup connection is terminated when the LMI declares the primary DLCI active, and the access unit drops DSR (data set ready), signaling the backup device to disconnect.

# Management Control and IP Addressing

# 2

This chapter contains the steps needed to provide management connectivity to the access unit. You need to select and configure:

- A method of local management connectivity for access units.
- A method for end-to-end management connectivity across the network.
- An IP addressing scheme that fits the local and end-to-end management connectivity methods.

## Configuring Local Management Control

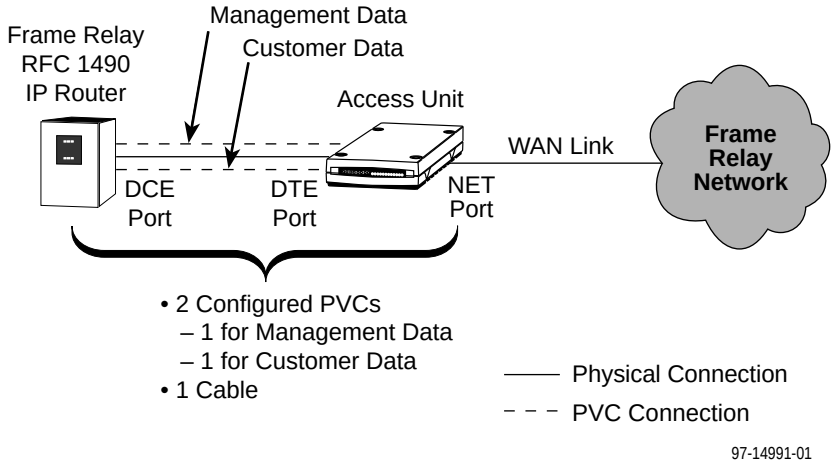
When managing the access unit locally, you can establish a management link in one of three ways. You can:

- Create a management DLCI using a DTE port.
- Create a separate management link through the COM port.
- Connect an external device (modem, LAN adapter, etc.) to the COM port.

## Configuring a Management DLCI Between the Router and Access Unit (RFC 1490 Router Using DTE Port)

The following configuration shows the management connection using an RFC 1490-compliant frame relay IP router connected to one of the access unit's DTE ports.

As shown below, in-band management is accomplished through the dedicated PVC between the frame relay router or FRAD and the access unit.




In this configuration, the access unit depends on the router for management connectivity. Only one DTE port is needed since the user data PVCs share the same port as the management PVC. No additional cables need to be purchased.

**NOTE:**

The router to be used for management must configure a PVC to support RFC 1490. This allows the access unit to recognize its IP data.

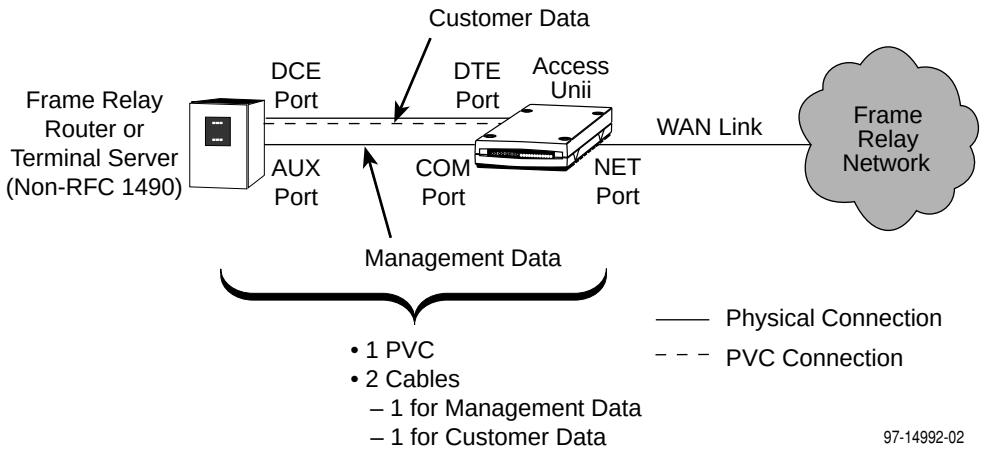
When a PVC is configured as the IP management link, the async terminal interface is accessible through Telnet. When this is the case, you also need to enable Telnet and FTP Sessions configuration options.

Menu selection sequence:
*Main Menu→ Configuration→ User Interface→ Telnet and FTP Sessions*

## Creating a Separate Management Link (Non-RFC 1490 Router Using COM Port)

A dedicated PVC can be configured to carry customer data over a DTE port, while management data is carried over the COM port. The illustration below shows a management link connected to the COM port for local access to a non-RFC 1490 router.

When the COM port is configured as the IP management link, the user interface is also accessible via Telnet. Although not shown in the illustration below, a LAN adapter can be connected to the COM port to provide Ethernet or Token Ring connectivity, or an async terminal (or other VT100-compatible) interface can be directly connected to the COM port, as well.




The configuration options below show what should be configured using a separate (out-of-band) management link. These configuration options are configured from the user interface based upon the Port Type selected, Asynchronous or Synchronous.

Menu selection sequence:
*Main Menu→ Configuration→ User Interface→ Communication Port*

**Port Use Set to Terminal and Port Type Set to Asynchronous**

— Data Rate (Kbps)

— Character Length

— Parity

— Stop Bits

— Ignore Control Leads

— RIP

**Port Use Set to Net Link and Port Type Set to Synchronous**

— Clock

— Data Rate (Kbps)

See Table 4-9 in Chapter 4, *Setting Up*.

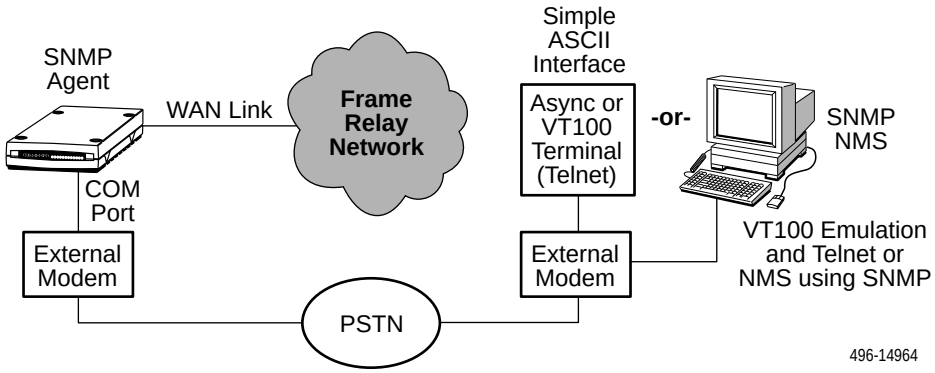
When the communication (COM) port is configured as the IP management link, the async terminal interface is accessible through Telnet. When this is the case, you also need to enable Telnet and FTP Sessions configuration options.

Menu selection sequence:
*Main Menu→ Configuration→ User Interface→ Telnet and FTP Sessions*

See Table 4-11 in Chapter 4, *Setting Up*.

## Configuring an External Device (Connected to the COM Port)

The access unit can be managed remotely by connecting an external device like a modem or PAD (packet assembly/disassembly) facility to the COM port.




Using this out-of-band example, configure call processing using the following pertinent configuration options, configured from the user interface.

Menu selection sequence:
*Main Menu→ Configuration→ User Interface→ External Device (COM Port)*

- External Device Commands
- Dial-In Access
- Connect Prefix
- Port Usage

See Table 4-10 in Chapter 4, *Setting Up*.

If connecting to an external device like a LAN adapter, configure the Communication Port Link Protocol for PPP.

Menu selection sequence:
*Main Menu→ Configuration→ User Interface→ Communication Port* and
*Main Menu→ Configuration→ Management and Communication*, respectively.

# Configuring End-to-End Management Control

When managing the access unit remotely, you can establish a management link across the network in one of three ways. You can:

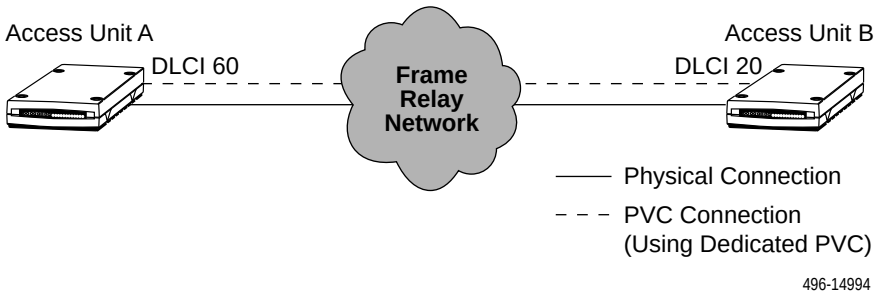
- Use a dedicated DLCI or PVC.
- Use a shared PVC (embedded DLCI).
- Use RFC 1490 routers for transparent management control.

## Management Control Using a Dedicated DLCI

The DLCI is the local network address of a PVC link. The DLCI at the source of a link and the DLCI at the destination of the link, along with all the DLCIs inside the network, make up the path that is the PVC; that is, the PVC links DLCIs at each end of the link.

There are two configured PVCs through the network:

- One for management data
- One for customer data




As shown in the example, in-band management is accomplished through the dedicated PVC between the two access units. Management data for Access Unit B goes to Access Unit A, which then routes it into the dedicated PVC between the access units. Only management data is carried over the PVC: source DLCI 60 to destination DLCI 20.

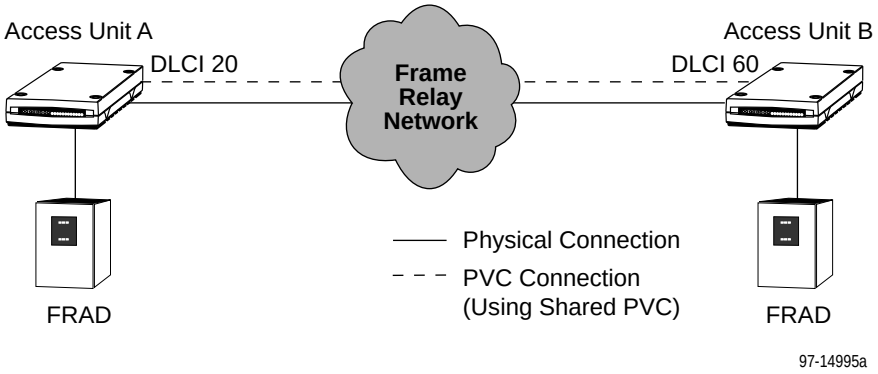
See *Frame Relay Switching Application* in Chapter 3 for a DLCI-linking example.

## Management Control Using Circuit Multiplexing (EDLCI)

In the configuration below, the access unit's management data is multiplexed with customer data onto a single PVC, sharing the same PVC: source DLCI 20 to destination DLCI 60. This is the preferred method.

There is one configured PVC through the network:

- A shared PVC for management and customer data



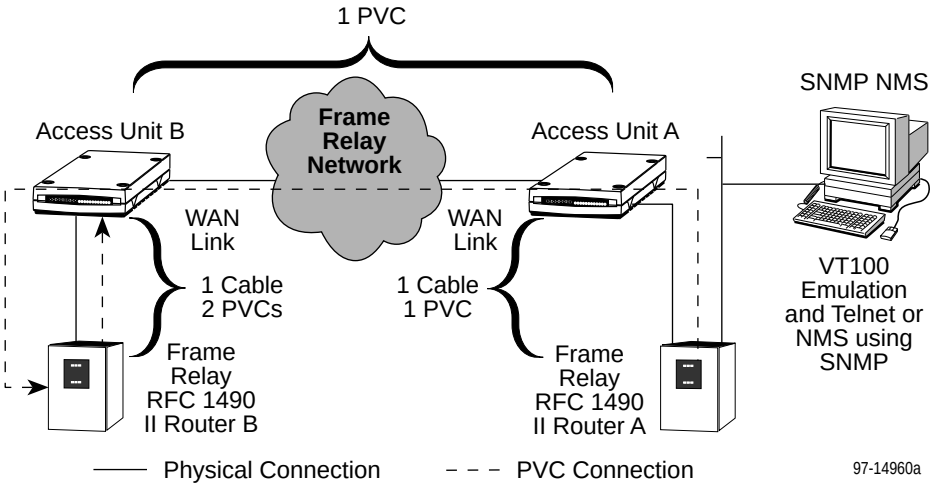

By identifying DLCIs carrying management data, higher priority can be given to DLCIs carrying customer data. You can configure the management embedded DLCI (EDLCI) to set the DE (discard eligible) bit. When the network encounters traffic congestion, it discards data from the DLCIs already marked discard eligible.

See *Frame Relay Switching Application* in Chapter 3 for a DLCI-linking example.

## Transparent Management Control Using RFC 1490 Routers

The access unit can be managed locally via in-band management channels using a frame relay PVC that is configured on a DTE port. When managing the access unit remotely, the access unit does not route IP traffic to the remote access unit. Instead, it is transparently passed through the access unit as part of customer data. The router then forwards the management data back to the access unit on the dedicated management DLCI configured between the router and the DTE port of the access unit.

The configuration below shows both local and remote management across the network. Management data is being routed from frame relay RFC 1490 IP Router A to RFC 1490 IP Router B, then being redirected by the router to Access Unit B. Both management and customer data are carried over the same PVC; a separate, dedicated management PVC is not required.



# Selecting an IP Addressing Scheme

You can select from many IP addressing schemes to provide SNMP NMS connectivity. When selecting a scheme, keep the following in mind:

- Because connection to remote devices is through PVCs, if desired, you can assign IP addresses and subnet masks to each PVC individually.
- Avoid multiple management PVC connections between the same two devices to prevent routing loops.
- Assign IP addresses on a per-interface or access unit basis.
- Although routing information is automatically passed between interconnected access units from the network side, make sure to set a route to the subnet(s) in the NMS's or local router's routing table.

  The gateway to subnet(s) is through the access unit connected to:

  — The LAN (using a LAN adapter), or

  — To a router's, terminal server's, or NMS's direct PPP (point-to-point protocol) or SLIP's (link-layer protocol for IP traffic) serial connection, or

  — The router's DTE port using a local PVC.
- Be aware that each access unit's routing table supports a maximum of 300 routes, even though a single route is all that is needed to reach every device on a subnet.
- Have a default route set only for devices directly connected to the NMS's COM port.
- Allow any legal host address for a given subnet; the address choice within the subnet is not important to the unit, but it should be selected in conjunction with all IP addressing for the subnet.

**NOTE:**

When dealing with IP addressing, your Information Systems (IS) department needs to be involved since they typically dictate the IP addressing scheme used in an organization.

# IP Addressing Scheme Examples

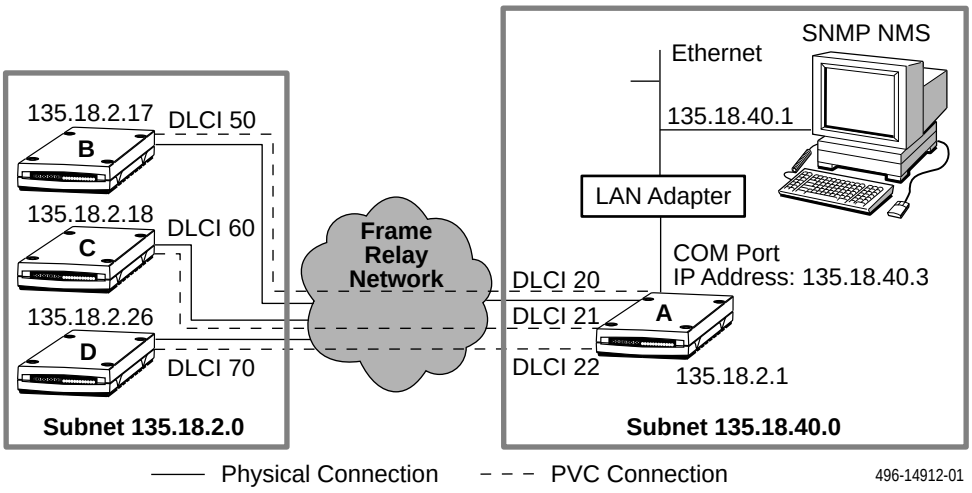
The following examples describe some typical network scenarios; they are not the only scenarios that can be used. The subnet mask shown for each access unit is 255.255.255.0.

## Direct PVCs to Remote Access Units

In this example, Access Unit A is connected to:

- The NMS at the central site
- Each remote access unit through a management PVC

The illustration below shows three separate management PVCs, one for each remote access unit.

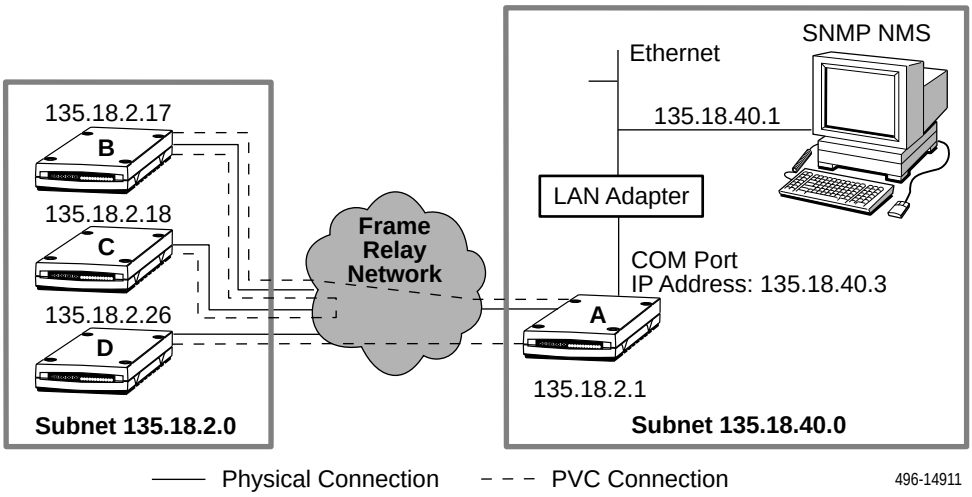


## Routing to Remote Access Units on the Same Subnet

In this example, Access Unit A is connected to:

- The NMS at the central site
- Remote access units through management PVCs

The illustration below shows two management PVCs at the central site, with Access Units B and C connected through one management PVC.



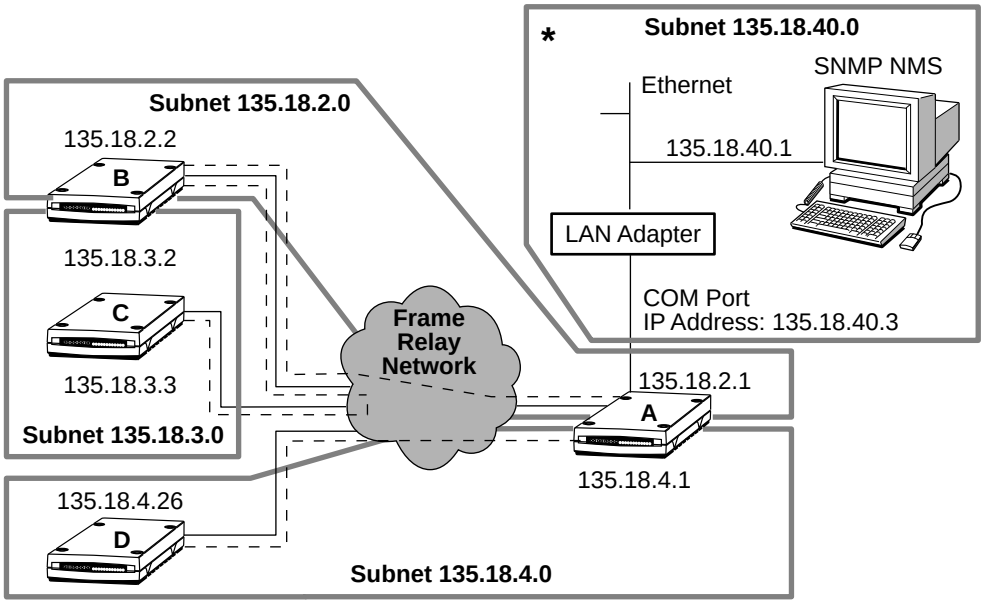
## Routing to Remote Access Units Using Different Subnets

In this example, Access Unit A is connected to:

- The NMS at the central site
- Two remote access units through management PVCs

The illustration below shows two management PVCs, with Access Units B and C connected through one management PVC. By configuring a different IP address and subnet for each management PVC:

- Access Units B and C share a subnet: 135.18.3.0
- Access Units A and B share a different subnet: 135.18.2.0
- Access Units A and D share yet another subnet: 135.18.4.0




* This subnet connection can be to any of the following:
  - SNMP NMS via the COM Port
  - LAN adapter via the COM Port
  - Frame relay RFC 1490 IP router via the DTE Port
  - Frame relay non-RFC router via AUX port-to-COM port
  - Terminal server via the COM Port

497-14913-01

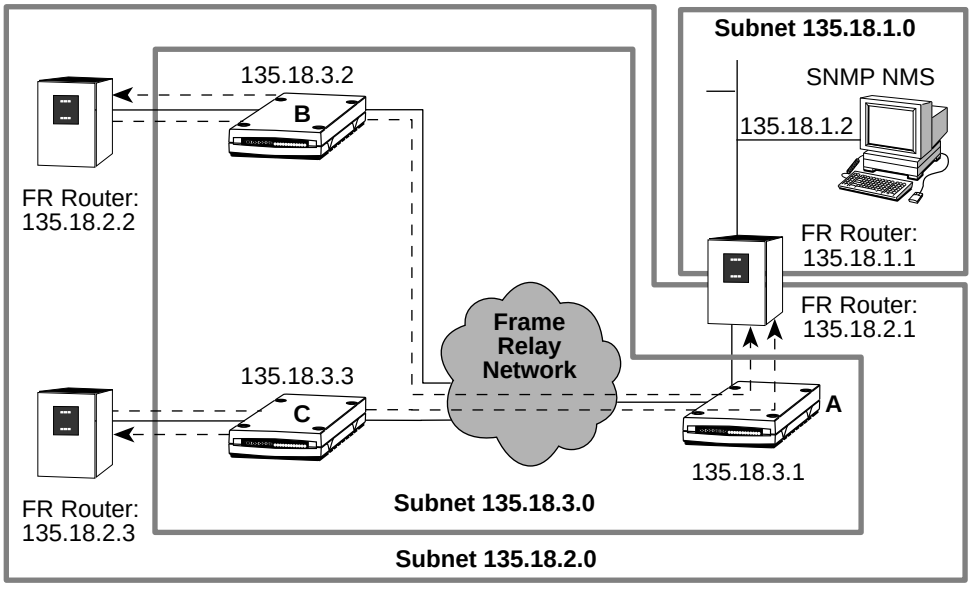
## Routing to Remote Access Units Using Routers

In the following examples, the access unit at the central site is connected to:

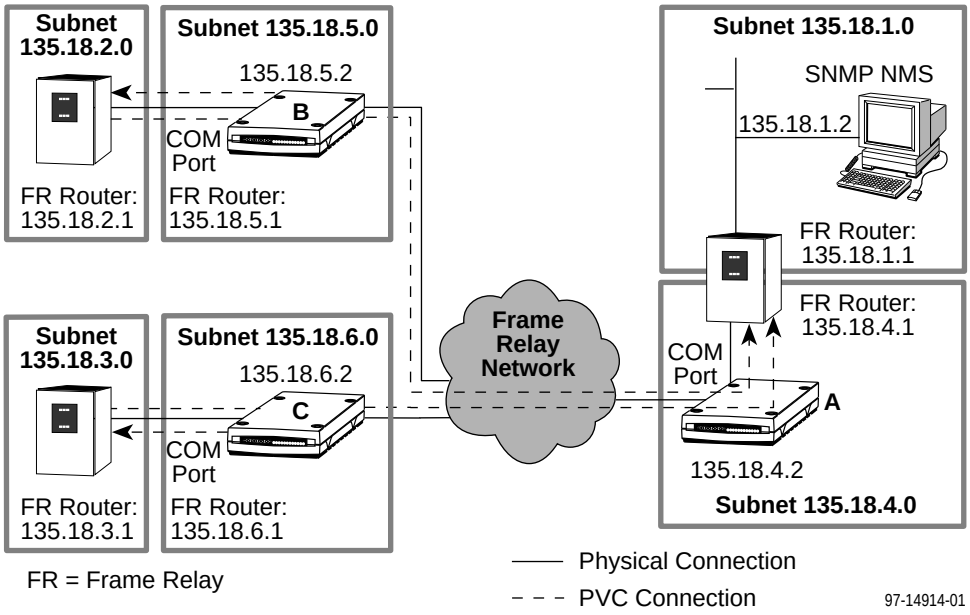
- A router (instead of a LAN connection)
- The router is connected to the NMS
- The router's additional serial or AUX port connection is not used for management
- No additional network PVCs are required

In the following examples, data is not routed by the access units, and management PVCs are not configured between them. Instead, management data for the remote access units is routed through the routers, with management PVCs configured between the routers and access units. Connection is via the existing DTE cable, between the router's DTE interface and the access unit.

The illustration below shows all access units on the same subnet, and all routers on the same subnet.



The following illustration is a more complex example in which each access unit is on its own subnet, having a subnet mask of FF.FF.FF.00. This subnet is independent of the subnet on the LAN supported by the local router.




## Assigning IP Addresses and Subnet Masks

Once you select an IP scheme, assign an address (or addresses) to the access unit.

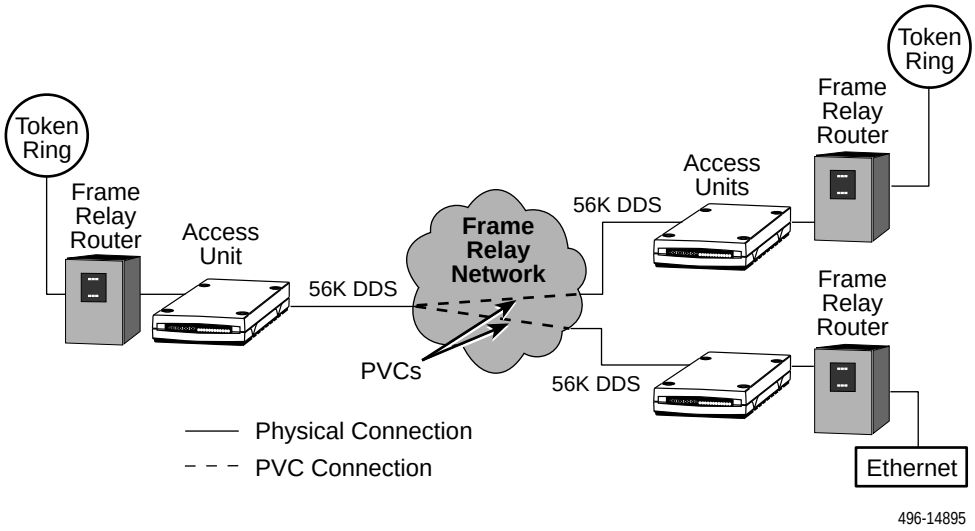
| If using . . . | Then . . . |
|---|---|
| COM port as a management interface | Assign the COM port address and net mask.<br>Menu selection sequence:<br>*Main Menu→ Configuration→ Management & Communication→ Communication Protocol* |
| COM port connected to an external modem | Configure an IP address and subnet mask to dial out traps using the alarm directory.<br>Menu selection sequence:<br>*Main Menu→ Configuration→ Alarm*<br>Or, configure the IP address and subnet mask.<br>Menu selection sequence:<br>*Main Menu→ Configuration→ Management & Communication→ Communication Protocol* |
| Frame relay PVCs to pass management data | Assign IP addresses and net masks to each PVC (to the node IP address if only one IP address per unit is desired).<br>Menu selection sequence:<br>*Main Menu→ Configuration→ Management & Communication→ Logical Communication Links* |

# Typical Applications

# 3

## DDS Access-to-Frame Relay Application

The following configuration shows typical DDS access to the frame relay service, with each FrameSaver access unit connected to a frame relay router.




In this example, the access units use their physical connection to the DDS network to gain access to the frame relay network via logical PVC connections. Access to the DDS network is through the unit's RJ48S interface.

FrameSaver access units operate at 56 kbps full-duplex (as shown above), or 64 kbps clear-channel operation if available in your area.

# Mixing Access Units in Applications

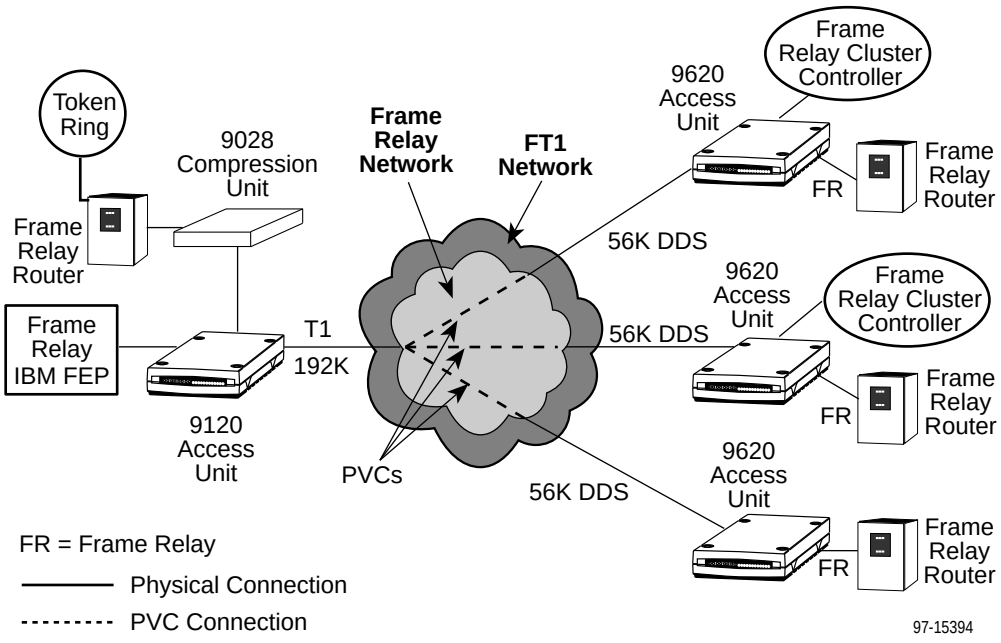
Deciding which frame relay access unit is needed at a central or remote site is a matter of evaluating the site's traffic volume to determine the amount of network access required: 56/64 kbps or FT1/T1.

One of the most common and practical applications for frame relay access units is to use a 9120 T1 frame relay access unit at the central site and 9620 frame relay access units at most remote sites.

This arrangement provides the greater speed and capability needed for high-volume central site applications, while allowing each remote site to have a router for email, etc., and a cluster controller for SNA traffic.

The example that follows shows this application, using a 9120 access unit at the central site, with remote sites using 9620 access units.

- At the central site, the 9120 access unit is designed to support up to 80***** remote sites, requiring a high degree of aggregation/deaggregation. In typical applications, a circuit-multiplexed PVC is expected from each remote unit containing PVCs from each data port, plus one PVC for management.
- At remote sites, three multiplexed DLCIs from each access unit are aggregated onto one PVC going through the frame relay network to the central site, each access unit's multiplexed DLCI containing traffic from its two data ports, with one DLCI for management.



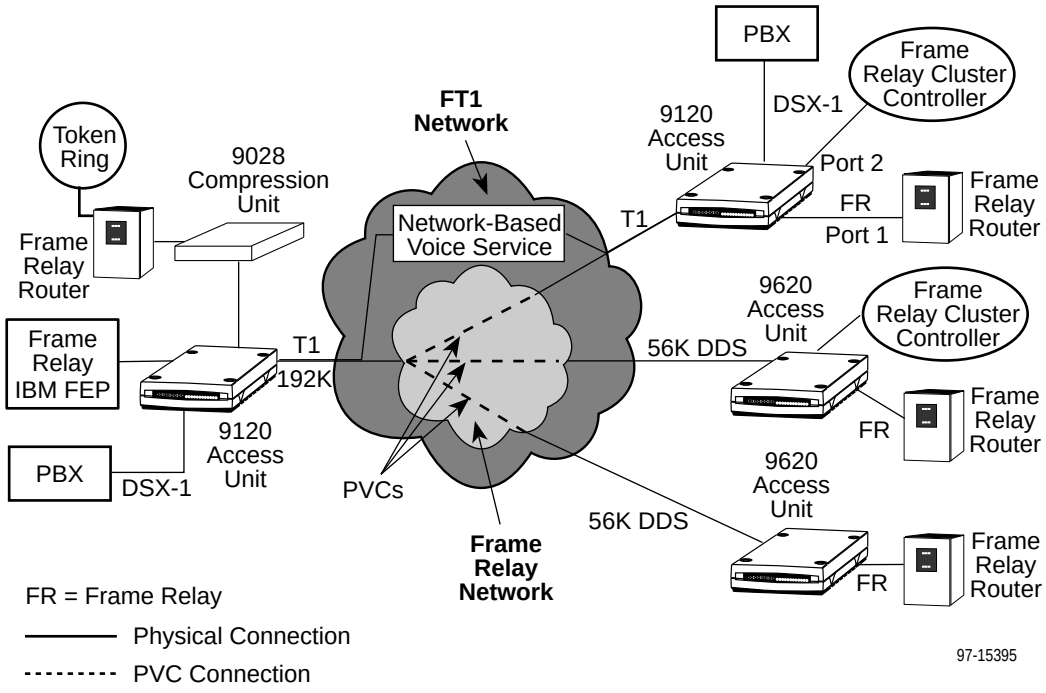

* If only one port is used per remote 9620 access unit and management DLCIs are not always used (e.g., management through the router at the remote site), the 9120 access unit could handle more than 80 remote sites. It could support up to 321 DLCIs, with up to 81 management DLCIs.

Circuit multiplexing is a proprietary method that provides the ability to multiplex frame relay frames coming from multiple DLCIs onto a single DLCI, sharing a single PVC connection.

As shown in the example, central site data compression is provided through a 9028 compression unit (CU), which is connected to the 9120 access unit's COM port. The 9028 CU is a high-performance, frame relay-compliant, fractional T1 (FT1) processor that provides compression rates up to 4-to-1. It was developed to work in conjunction with a 9120 access unit to provide high-speed compression/decompression capability.

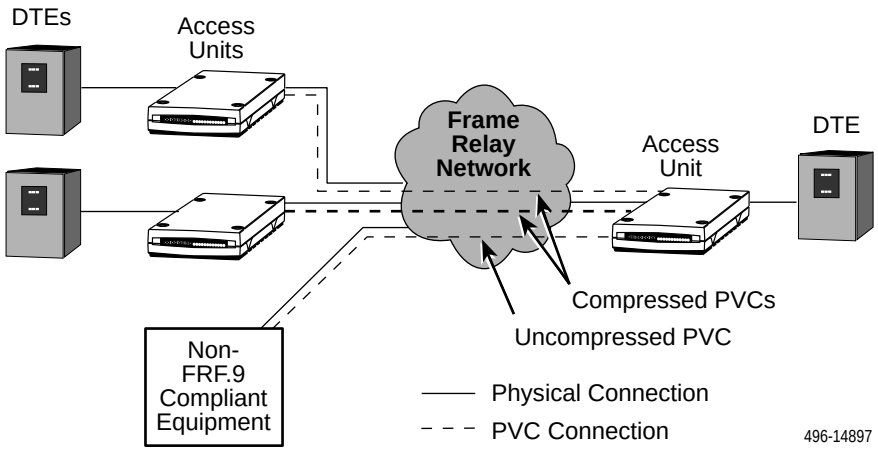
At the remote sites, the access unit's compression feature is used, which provides data compression on Port 1.

Refer to the *9028 Compression Unit, Installation and User's Manual* for more information.



# Data Compression Application

The application below shows the PVCs between two FrameSaver access units configured for data compression.




The example shows a PVC coming from a non-FRF.9-compliant device that is configured for non-compression since the other vendor's equipment probably will not interoperate with the FrameSaver access unit.

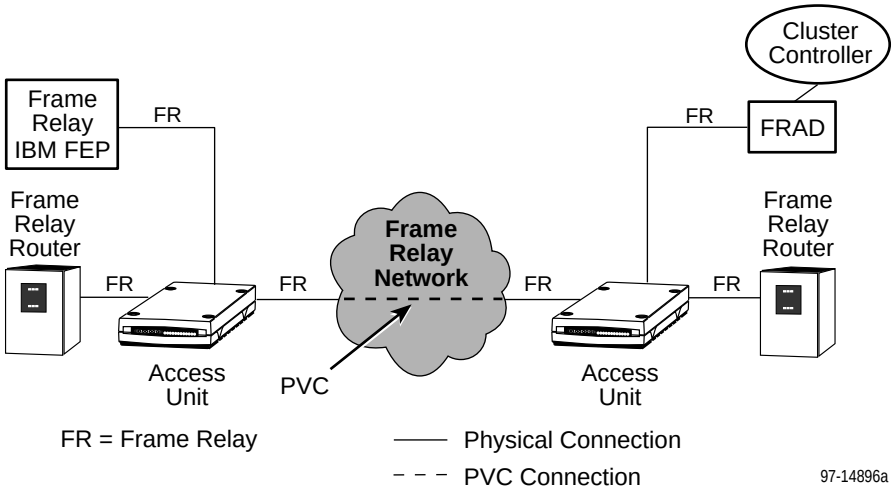
See *Configuring Port 1 for Data Compression* in Chapter 4.

# Frame Relay Port Aggregation and Circuit Multiplexing Application

The FrameSaver access unit allows two ports to share a single frame relay link, which is called *port aggregation*. Since only one physical network connection is required, port charges are reduced. In addition, each port can be configured for different inbound and outbound CIR enforcement methods, and each PVC on each port is configured for separate CIRs and burst rates.

When FrameSaver access units are at each end of the circuit, the access unit also provides the ability to multiplex the data of multiple DLCIs or data coming from multiple frame relay devices onto a single network DLCI. This feature is referred to as *circuit multiplexing*.

Both aggregation and multiplexing use the following network configuration.




The example shows frame relay data coming in over Ports 1 and 2, with the frames being multiplexed onto a single network connection. PVCs are aggregated in the same manner.

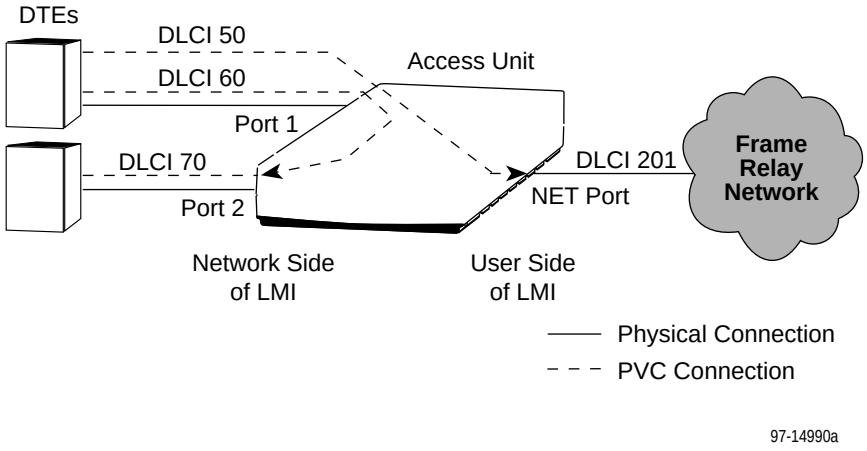
This sharing of PVCs (i.e., multiplexing user DLCIs or management data/frames with user data/frames) is a proprietary method. When using this method, you must either:

- Specify that you are using the PVC in this way, and you can configure management data to be marked discard eligible (DE) so that user data has priority (selected from the PVC Connection Entry screen), or
- Configure a committed information rate (CIR) great enough that both management and user data/frames can be carried by the PVC (selected from the DLCI Record Entry screen).

# Frame Relay Switching Application

Any DLCI on any port can be cross-connected to any DLCI on any other port. In addition, any port can be configured to support either the user or network side of the UNI.

The following example shows how the FrameSaver access unit is used as a limited frame relay switch.




The following table provides an example, using the DLCIs shown above, illustrating how DLCI connections are configured.

| Source Interface | Source DLCI | Destination Interface | Destination DLCI |
|---|---|---|---|
| Port 1 | DLCI 50 | Network (NET) | DLCI 201 |
| Port 1 | DLCI 60 | Port 2 | DLCI 70 |

This example shows DLCIs coming in over each DTE port. For each port, you configure each DLCI; that is, you configure a separate PVC connection for each in-coming DLCI.

Menu selection sequences:
*Main Menu→ Configuration→ PVC Connections→ New* **or**
*Main Menu→ Configuration→ Ports→ DLCI Records→ New*

# Using Configuration Shortcuts

When the FR (frame relay) Discovery feature is used, DLCI configuration and PVC connection occur automatically when the network interface is configured as the user side of LMI, the usual configuration. The FrameSaver access unit “discovers” network DLCIs from the network LMI status response message. Network and Port interface DLCIs are created automatically to correspond with DLCIs discovered from the network, and the access unit connects them. All automatically-configured DLCIs are multiplexed.

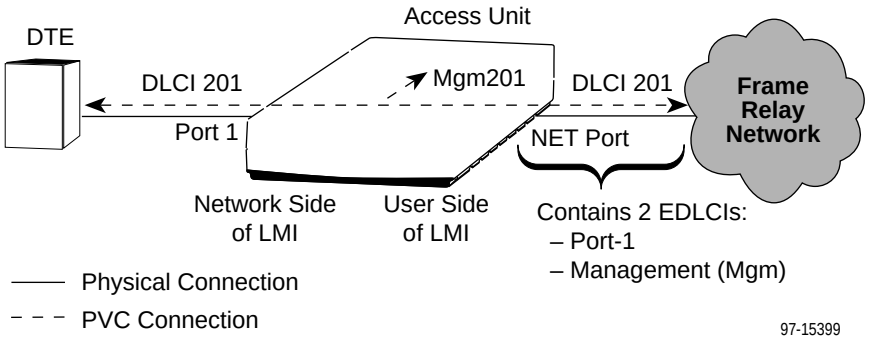
When management PVCs are multiplexed with data, two or three DLCIs are created from the network DLCI – one or two matching DLCIs for data (one per port) and another for management (Mgm) information.

If the unit at the other end of the network PVC is *not* a FrameSaver access unit (9x2x models), FR Discovery mode should be set to NetOnly, 1Port, or Disable; only one port can be used and no management DLCIs can be created. In addition, PVC diagnostic tests cannot be run without disrupting data. This is because only FrameSaver models currently support port and PVC multiplexing, and PVC diagnostics.

Using an example similar to the previous illustration, the following shows the DLCI records and PVC connections created when a frame relay discovery method is selected. The tables illustrate the automatic configuration that takes place within the access unit.

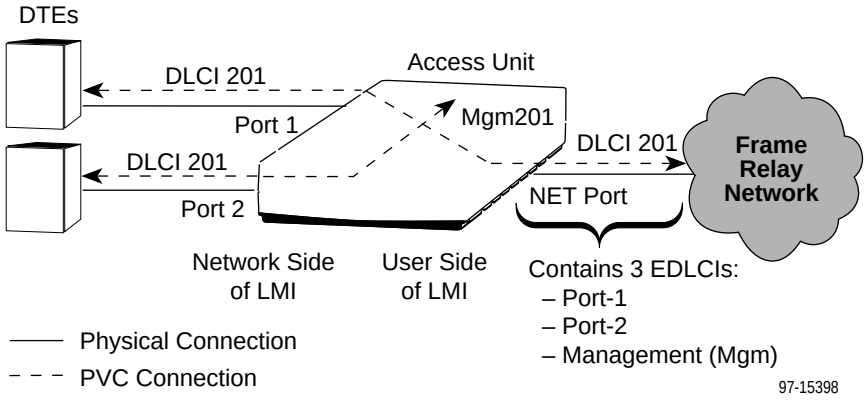
Refer to *Using Configuration Shortcuts* in Chapter 4 for additional information.

This example shows the 1-port management application (1MPort).



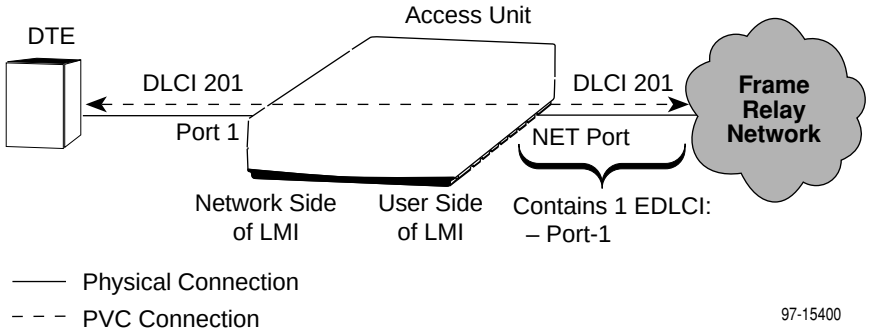

| FR Discovery Selection | Source Interface | Source DLCI | Primary Destination Interface | Primary Destination DLCI | Primary Destination EDLCI |
|---|---|---|---|---|---|
| One port with Management | Port-1 | DLCI 201 | Network (NET) | DLCI 201 | EDLCI 0 |
| | Internal | Mgm201 | | | EDLCI 2 |

The following shows the 2-port management configuration (2MPort).




| If the FR Discovery Selection is . . . | Source Interface | Source DLCI | Primary Destination Interface | Primary Destination DLCI | Primary Destination EDLCI |
|---|---|---|---|---|---|
| Two ports with Management | Port-1 | DLCI 201 | Network (NET) | DLCI 201 | EDLCI 0 |
| | Port-2 | DLCI 201 | | | EDLCI 1 |
| | Internal | Mgm201 | | | EDLCI 2 |

This example shows the 1-port non-management configuration (1Port).




| If the FR Discovery Selection is . . . | Source Interface | Source DLCI | Primary Destination Interface | Primary Destination DLCI | Primary Destination EDLCI |
|---|---|---|---|---|---|
| One port with No Management | Port-1 | DLCI 201 | Network (NET) | DLCI 201 | EDLCI 0 |

# Backup Applications

Backup provides continuing service in case of a network, LMI, or PVC failure. Being a frame relay aware product, the FrameSaver access unit continually monitors the frame relay physical and logical links to detect these failures.

If the automatic backup feature is enabled, backup occurs immediately and automatically when a failure is detected, without operator intervention or the delay of waiting for the LMI to time out when using a router for backup.

To provide backup, the FrameSaver access unit must be equipped with either an internal ISDN BRI DBM connected to the ISDN through the backup (BKP) interface, which provides an ISDN U-interface, or an external backup device connected to a DTE port.

- Directories or profiles must be set up.
- Alternate destination options must be configured.
- One end of the circuit must be configured to originate backup, while the other end must be configured to answer a backup call.
- One side of LMI must be configured for the Network Side (LMI Personality) on the alternate destination link, and the other end must be configured for User Side.

Here is how backup works:

1. When a network, LMI, or PVC failure is detected, the FrameSaver access unit generates an alarm, which triggers an SNMP Trap.
2. If the unit is configured for automatic backup and an alternate destination circuit has been configured, the FrameSaver access unit places a call to the answering device at the other end.
3. Once a connection is established between backup devices or DBMs, the access unit switches data to the backup link/alternate path that has just been established.

   All reconfiguration occurs automatically within the unit, entirely transparent to the connected DTE.

For circuit restoration:

1. When the FrameSaver access unit detects that normal service has been restored, the access unit clears the alarm and SNMP Trap.
2. Data is switched back to its original path.

The backup link is always disconnected when one of the units of the backup link physically disconnects, when the backup link LMI has timed out, or when all alternate DLCIs on the backup link become inactive. If the backup link is disconnected but the failure is still detected, the unit continues to try and re-establish the connection until the failure is no longer detected.

The following sections discuss two backup applications: backing up to the primary destination node, and backing up to an intermediate/neighboring node. When backing up to a destination node, two methods can be used:

- An alternate network like ISDN or POTS (plain old telephone service) can be used, bypassing possible frame relay network problems. This allows the units to completely bypass network problems, and gives the operator more control
- Access to ISDN or POTS lines may be provided by the service provider through its own network.

Either way, the ISDN BRI DBM supports a variety of backup schemes. The access unit itself supports various LMI types, provides switching capability, and performs continuous monitoring of the frame relay physical and logical link's condition. Combined with the ISDN BRI DBM's capabilities, better, faster, and easier backup can be achieved than when relying upon a router for backup.

Refer to:

- *About Backup* in Chapter 1 for information about the philosophies behind development of the backup feature, and for additional information about using an internal ISDN BRI DBM or an external backup device.
- *Setting Up* in Chapter 4 for assistance configuring the backup feature.
- *Backup Security* in Chapter 6 for information about the security provided data over the alternate/backup path.

## Backing Up to the Primary Destination Node

Many times, it is desirable to backup to the ultimate destination node directly using an alternate network like ISDN or POTS (plain old telephone service). This method allows the FrameSaver access units to bypass network problems completely, and gives the operator more control.

The FrameSaver access unit provides the features to achieve this goal.

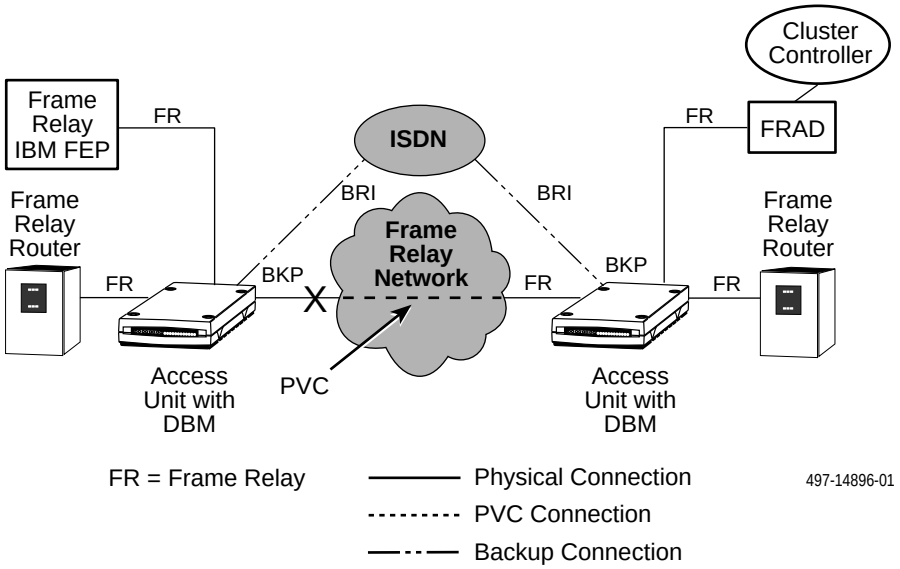
- **Regeneration of LMI** – When the access units are configured so that one end of the circuit is set to the network side, and the other is set to the user side of LMI on the alternate destination link (see LMI Personality), the access units set up a frame relay link over ISDN or POTS line when the frame relay network connection fails.

  This ensures that no matter what type of service is used for the alternate/backup path, the units can establish a frame relay user-to-network interface (UNI) between them.

- **Alternate Destination concept** – As part of this concept, the DLCI (data link connection identifier) on the alternate destination link can be a different number than the primary destination link. DLCI numbers are assigned by the local service provider, and they might not have significance to the destination unit, and DLCI numbers must match at both ends of the circuit.

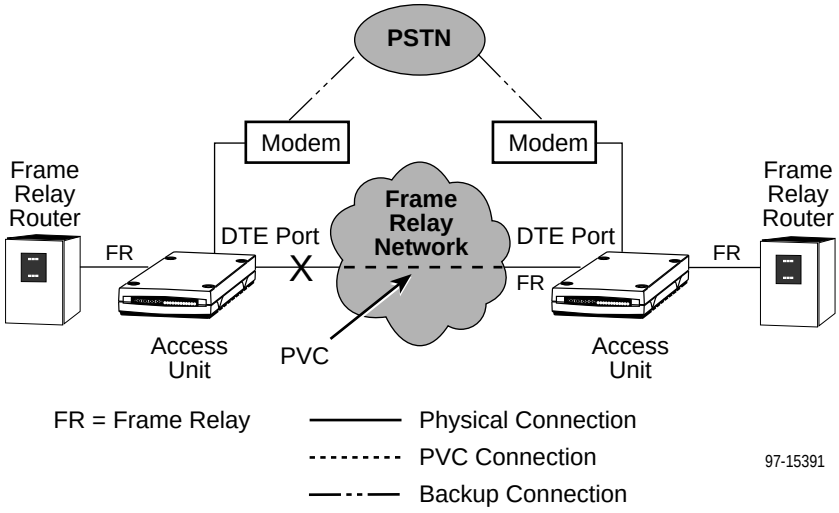
  Configuring an alternate destination link and DLCI number allows a direct backup connection to be established by cross-matching a source unit's DLCI number to an alternate destination unit's DLCI number.

The example below shows an application using an ISDN BRI DBM to back up directly to the primary/final destination.

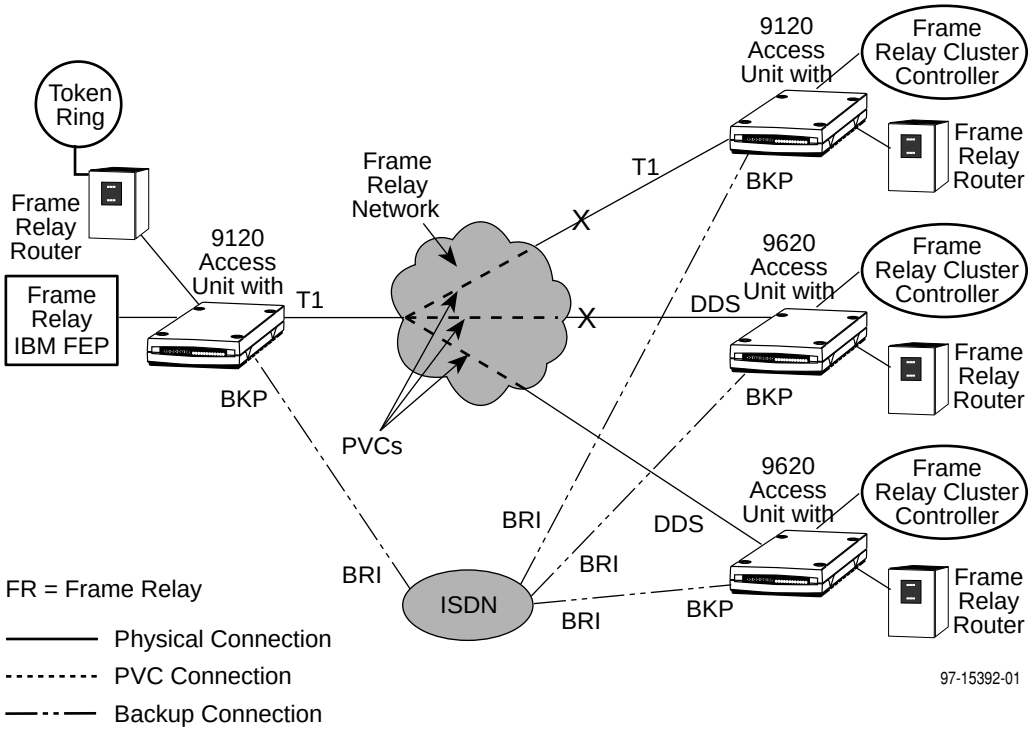



The backup connection to the ISDN is via the backup (BKP) interface.

In the following example, an external backup device creating the backup link is a modem, which is connected to one of the FrameSaver access unit's DTE ports. The alternate path is through the PSTN (public switched telephone network).




This illustration of a FrameSaver access unit directly backing up to the final destination shows a network failure, with backup being accomplished using the alternate networks, ISDN or PSTN.



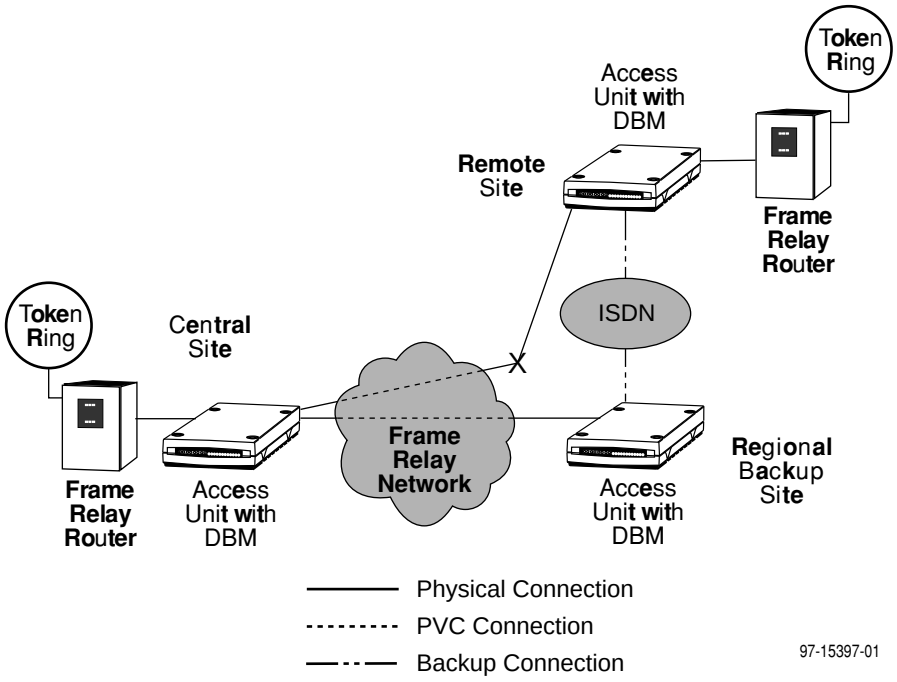
The following table shows how these access units should be configured when using ISDN BRI DBMs for backup. It assumes the ISDN BRI DBM physical, frame relay, DLCI records, and ISDN Call Profiles have been set up. Refer to the *Setting Up an ISDN BRI DBM* section of Chapter 4, *Setting Up*, for additional information.

| **Remote Access Unit with ISDN BRI DBM** | **Primary Destination Access Unit with ISDN BRI DBM** |
|---|---|
| ***ISDN BRI DBM's B Channel Physical Options, Table 4-4*** | |
| ■ BRI-B1 set to Enable<br>■ Originate or Answer set to Originate | ■ BRI-B1 set to Enable<br>■ Originate or Answer set to Answer |
| ***ISDN BRI DBM's B Channel Frame Relay Options, Table 4-5*** | |
| ■ LMI Personality set to User Side | ■ LMI Personality set to Network Side |
| ***PVC Connections Options, Table 4-7*** | |
| Source<br><br>Applicable data source | Source<br><br>Applicable data source |
| Primary Destination<br>■ Link set to Network<br>■ DLCI (to the primary destination unit)<br>■ EDLCI | Primary Destination<br>■ Link set to Network<br>■ DLCI (to the remote unit)<br>■ EDLCI |
| Alternate Destination<br>■ Link set to BRI<br>■ Profile Called ID (to the primary destination unit)<br>■ DLCI<br>■ EDLCI | Alternate Destination<br>■ Link set to BRI<br>■ Profile Calling ID (from the remote unit)<br>■ DLCI<br>■ EDLCI |
| ***Auto Backup Criteria Options, Table 4-18*** | |
| ■ Auto Backup set to Enable | ■ Auto Backup set to Enable |

## Backing Up to a Neighboring Node

Sometimes it is desirable to backup to a neighboring node like a regional node (e.g., when the FrameSaver access unit is part of a mesh or partial-mesh network, or when only selected units are to place backup calls to the central site). When the regional node receives a call from its neighbor, the FrameSaver access unit switches the remote access unit's alternate destination traffic with its own primary traffic, then sends the traffic to the frame relay network.

The application example below shows a remote access unit backing up to a neighboring access unit, both equipped with an ISDN BRI DBM, using the Auto Backup feature. (In this example, the central site is equipped with an ISDN BRI DBM, but the DBM is not necessary for this application.)




Extra CIR for network DLCIs and/or additional network DLCIs must be provisioned with/by the network provider to implement this application.

- If multiplexed DLCIs are used, increase CIR for the network DLCIs between the regional and central sites to allow for the additional backup traffic (DLCIs plus the EDLCIs).
- If multiplexed DLCIs are not used, additional network DLCIs between the regional and central sites (the regional unit's DLCIs plus the remote unit's DLCIs) must be provisioned for use during backup.

The following table shows how these access units should be configured when using ISDN BRI DBMs for backup. It assumes the ISDN BRI DBM physical, frame relay, DLCI records, and ISDN Call Profiles have been set up. Refer to the *Setting Up an ISDN BRI DBM* section of Chapter 4, *Setting Up*, for additional information.

| Remote Access Unit with ISDN BRI DBM | Regional Access Unit with ISDN BRI DBM | Central Site Access Unit |
|---|---|---|
| ***ISDN BRI DBM's B Channel Physical Options, Table 4-4*** | | |
| ■ BRI-B1 set to Enable<br>■ Originate or Answer set to Originate | ■ BRI-B1 set to Enable<br>■ Originate or Answer set to Answer | n/a |
| ***ISDN BRI DBM's B Channel Frame Relay Options, Table 4-5*** | | |
| ■ LMI Personality set to User Side | ■ LMI Personality set to Network Side | n/a |
| ***PVC Connections Options, Table 4-7*** | | |
| Source<br>Applicable data source | Source[1]<br>■ Link set to BRI<br>■ Profile Calling ID (from the remote unit)<br>■ DLCI (to the remote unit's Alternate Destination DLCI)<br>■ EDLCI | Source<br>Applicable data source |
| Primary Destination<br>■ Link set to Network<br>■ DLCI (to the central unit)<br>■ EDLCI | Primary Destination<br>■ Link set to Network (to the central site 9120 or 9620)<br>■ Profile<br>■ DLCI (to the central site's Alternate Destination DLCI)<br>■ EDLCI | Primary Destination<br>■ Link set to Network<br>■ DLCI (to the remote unit)<br>■ EDLCI |
| Alternate Destination<br>■ Link set to BRI<br>■ Profile Called ID (to the regional unit)<br>■ DLCI<br>■ EDLCI | n/a | Alternate Destination<br>■ Link set to Network<br>■ DLCI (to the regional unit)<br>■ EDLCI |
| ***Auto Backup Criteria Options, Table 4-18*** | | |
| ■ Auto Backup set to Enable | n/a | ■ Auto Backup set to Enable |

[1] Only active when the remote unit calls and links with the regional unit. While inactive (waiting for a call), an alarm will be generated and the regional unit's alarm (ALM) LED will be lit.

# Setting Up

# 4

## Considerations When Setting Up

We recommend that you decide how to configure the FrameSaver access unit before actually configuring it. Appendix B, *Configuration Worksheets*, contains aids to help you configure the FrameSaver access unit. Print out a set as you make these determinations.

When setting up the FrameSaver access unit, you need to:

- Arrange for ISDN service if an ISDN BRI DBM is installed.
- Determine where PVCs will be required in your network. Refer to Chapter 3, *Typical Applications*, for assistance.
- Depending upon where a PVC is required and whether aggregation is needed, determine the number of management PVCs that will be needed.
- Decide how and when you will use the Data Compression feature. Refer to Chapter 1, *About the FrameSaver 9620*, for basic data compression concepts when using this feature.
- Determine whether you will be using the Configuration Shortcuts (auto-configuration) feature when setting up. Refer to *Using Configuration Shortcuts* on page 4-13.
- Decide how traffic congestion will be monitored, which CIR enforcement mode will be used: inbound or outbound, and how much CIR and excess burst size will be required (see *About Congestion Control* in Chapter 1).
- Determine whether you want alarms and SNMP traps generated, and how you would like them communicated to an ASCII terminal/printer or management system.

- Decide how you want to manage the unit, and choose a management configuration:
  - — Locally, through a PVC between the FrameSaver access unit and a router attached to the DTE port.
  - — Locally, through a direct connection to the user interface via an asynchronous terminal.
  - — Remotely, using dedicated or multiplexed PVCs for in-band management.
  - — Remotely, from a remote terminal via a modem or Telnet connection.
  - — Remotely, through an SNMP NMS, routers, or Internet devices.
- If managing the FrameSaver access unit using an SNMP NMS or Telnet, select an IP addressing scheme. Refer to Chapter 2, *Management Control and IP Addressing*, for sample IP addressing schemes.

## Selecting a Management Interface

Select one of the following management interfaces:

- Asynchronous terminal user interface – Over the FrameSaver access unit's COM port for local configuration and control when the system does not include an NMS.

  An asynchronous terminal is also required for initial setup to enable external management.
- Telnet access to the user interface – Over the FrameSaver access unit's COM port or through an in-band management channel (PVC).
- SNMP – Over the FrameSaver access unit's COM port using a modem or LAN adapter, or over the network interface or one of the DTE ports for in-band management channels using PVCs.

## Minimal Remote Configuration

At a minimum, the following configuration options must be set before deploying a a FrameSaver access unit to a remote site:

- Configure the Node IP Address and Node Subnet Mask (see Management and Communication configuration options, Communication Protocol, page 4-63).
- Enable SNMP Management (see Management and Communication configuration options, General SNMP Management, page 4-70).
- Enable Telnet Session (see Telnet and FTP Session configuration options, page 4-59).

# Recommended Order for Setup

Before starting, it is recommended that you print and/or copy the configuration worksheets that are provided in Appendix B and review the factory-set (default) options ahead of time. Reviewing and completing the configuration worksheets before you start configuring the unit will speed setup time.

The worksheets show the options that can be configured, with their factory-set (default) options in boldface type and in brackets. If a setting needs to be changed, you can mark the changes in one of two ways:

- Circle or write-in *only* the setting that needs to be changed from the default setting.
- Circle or write-in the setting for *each* configuration option.

To help you get started, the following sequence of activities is recommended when setting up for operation. Use the menu sequences shown to access the appropriate branch of the menu, as needed.

**Menu Sequences (1 of 6)**

| Steps for Setup | Menu Selection Sequence |
|---|---|
| 1. Set up an async terminal to access the user interface. | Configure terminal to be compatible with the user interface:<br>■ Speed or data rate set to 19.2 kbps.<br>■ Character length set to 8.<br>■ Parity set to None.<br>■ Stop Bits set to 1.<br>■ Flow Control set to None. |
| 2. Configure access to the user interface. | *Main Menu→ Configuration→ User Interface→*<br>■ *Communication Port*<br>■ *External Device (COM Port)*<br>■ *Telnet and FTP Sessions* |
| 3. Configure management communication. | *Main Menu→ Configuration→ Management and Communication→*<br>■ *Communication Protocol→*<br>– *Node IP Address (minimally)*<br>– *Node Subnet Mask (minimally)*<br>■ *Management PVCs* [1]<br>■ *General SNMP Management*<br>■ *SNMP NMS Security*<br>■ *SNMP Traps* |
| [1] Not necessary if auto-configuration is used and management access is through the frame relay network. | |

**Menu Sequences (2 of 6)**

| Steps for Setup | Menu Selection Sequence |
|---|---|
| 4. If LMI provided by the network provider is not ANSI Annex-D, configure LMI Protocol for the network interface. | *Main Menu*→ *Configuration*→ *Network*→ *Frame Relay*→ *LMI Protocol*→ *Standard or Annex-A* |
| 5. Select a configuration template so that only the appropriate port options appear for configuration. | *Main Menu*→ *Configuration Shortcuts*→ *Config Template*<br>■ *1Port*<br>■ *1Port-Compr*<br>■ *2Ports*<br>■ *2Ports-Compr*<br>■ *None* (default) |
| 6. Configure physical and frame relay options for each data port, the network interface, and the backup interface. | |
| – For each data port: | *Main Menu*→ *Configuration*→ *Ports*→ *[Port-1/Port-2]* →<br>■ *Physical*<br>■ *Compression* (Port 1 only)<br>■ *Frame Relay* |
| – For the network: | *Main Menu*→ *Configuration*→ *Network*→<br>■ *Physical*<br>■ *Frame Relay* |
| – For the ISDN BRI DBM, if installed: | *Main Menu*→ *Configuration*→ *ISDN BRI DBM*→<br>■ *Physical* [2]<br>■ *Frame Relay* |
| [2] Make sure one end of the circuit is configured to originate calls, while the other end is configured to answer calls. | |

**Menu Sequences (3 of 6)**

| Steps for Setup | Menu Selection Sequence |
|---|---|
| 7. If 1MPort is not the mode wanted for automatic configuration of DLCIs and PVCs, select another frame relay discovery mode. | *Main Menu*→ *Configuration Shortcuts*→ *FR Discovery*→<br>■ *1Port*<br>■ *1MPort* (default) [3]<br>■ *1Port-Compr*<br>■ *1MPort-Compr*<br>■ *2MPorts*<br>■ *2MPorts-Compr*<br>■ *NetOnly*<br>■ *Disable* |
| If using the FR Discovery feature, connect the network cable at this time, and allow the access unit to start configuring and cross-connecting DLCI records. | To view automatically-created DLCI records:<br>*Main Menu*→ *Status*→ *LMI Reported DLCIs*→ *Network* |
| 8. Configure DLCI records for each data port, network interface, and backup interface.[4] | |
| – For each data port: | *Main Menu*→ *Configuration*→ *Ports*→ *[Port-1/Port-2]*→ *DLCI Records* [1] |
| – For the network: | *Main Menu*→ *Configuration*→ *Network*→ *DLCI Records* [1] |
| – For the ISDN BRI DBM, if installed: | *Main Menu*→ *Configuration*→ *ISDN BRI DBM*→ *DLCI Records* |
| 9. Set up COM port call directories and ISDN call profiles. | |
| – If connecting to an external device (e.g., a modem) used for management via the COM port: | *Main Menu*→ *Control*→ *COM Port Call Directories* to create up to 5 directory phone numbers and one alarm directory phone number. |
| – If using an ISDN BRI DBM for dial backup: | *Main Menu*→ *Control*→ *ISDN Call Profiles* to create up to 3 ISDN call profiles. |

[1] Not necessary if auto-configuration is used and management access is through the frame relay network.

[3] Provides access so that the unit can be configured remotely.

[4] If using the Auto-Configuration feature, make sure you do not duplicate DLCIs.

**Menu Sequences (4 of 6)**

| Steps for Setup | Menu Selection Sequence |
|---|---|
| 10. Configure local management DLCIs and PVCs (e.g., between the access unit and the router on the DTE port). Local management DLCIs and PVCs cannot be configured automatically. | *Main Menu→Configuration→ Management and Communications→ Management PVCs* |
| 11. If manually configuring DLCIs and PVCs (not using the automatic configuration feature), configure them at this time, starting with DLCIs. | *Main Menu→Configuration→ Ports→ [Port-1/Port-2] → DLCI Records* |
| 12. Configure PVC connections between DLCIs. | *Main Menu→ Configuration→ PVC Connections→ New*<br>■ *PVC Connections*<br>– Source [1]<br>– Primary Destination [1]<br>– Alternate Destination [5] |
| 13. Complete configuring management of the access unit, if needed. | *Main Menu→ Configuration→ Management and Communication→*<br>■ *Communication Protocol*<br>■ *Management PVCs* [1]<br>■ *General SNMP Management*<br>■ *SNMP NMS Security*<br>■ *SNMP Traps* |
| 14. Configure alarm and SNMP trap notification. | *Main Menu→ Configuration→ Alarm* |
| 15. Configure test timeout and duration. | *Main Menu→ Configuration→ General* |
| 16. Set up logins if using security.[6] | *Main Menu→ Control→ Administer Logins→ New* |
| 17. Enter device identification information. The device name appears at the top of each screen. | *Main Menu→ Control→ Device Name* |
| 18. Configure for automatic backup. | *Main Menu→ Configuration→ Auto Backup Criteria → Auto Backup→ Enable* |

[1] Not necessary if auto-configuration is used and management access is through the frame relay network.

[5] An alternate destination must be specified for backup and must be configured after FR Discovery has occurred.

[6] Logins and screen setup can be created before or after setup and configuration of the access unit.

**Menu Sequences (5 of 6)**

| Steps for Setup | Menu Selection Sequence |
|---|---|
| 19. Verify connections. | |
| – For the network and each data port:<br>Refer to Chapter 4, *Displaying System Information*, in the User's Guide to interpret status messages. | *Main Menu→ Status→ System and Test Status→ Health and Status column* |
| – For an external backup device to place a call manually:<br>Refer to *Manual Dial Backup* in Chapter 5 for additional information. | Disable a primary destination network DLCI on the data port connected to the external backup unit. Do this for units at both ends of the circuit. An alternate destination must have been specified.<br>*Main Menu→ Configuration→ Data Ports→ [Port-1/Port-2]→ DLCI Records→ Modify→ DLCI Number→ DLCI Status→ Disable* |
| – For an ISDN BRI DBM, if installed:<br>Refer to *Manual Dial Backup* in Chapter 5 to verify dial backup operation when passing data. | This procedure is for testing without passing data in order to verify connections.<br>1. Disable all ISDN Call Profiles but the Destination to be tested, or make sure the first ISDN Call Profile that is enabled is the one to be tested.<br>*Main Menu→ Control→ ISDN Call Profiles*<br>2. Verify that the B channel to be tested is enabled and its frame relay Link Status configuration option is set to Disable. If not, change the Link Status setting and save.<br>*Main Menu→ Configuration→ ISDN BRI→ [BRI-B1/BRI-B2] Frame Relay*<br>To test the connection:<br>3. Enable frame relay Link Status for the B channel to be tested.<br>*Main Menu→ Configuration→ ISDN BRI→ [BRI-B1/BRI-B2] Frame Relay→ Link Status→ Enable*<br>This causes the Destination contained in the first enabled ISDN Call Profile to be called and LMI to be established (no DLCIs will be established, but LMI messages will be exchanged). |

**Menu Sequences (6 of 6)**

| Steps for Setup | Menu Selection Sequence |
|---|---|
| 20. Verify connections. *(cont'd)*<br><br>– For an ISDN BRI DBM, if installed: | To verify the connection:<br>4. View the DBM Interface Status screen (Line Status should show Active. Operating Mode for the B channel should be Active and the Active Call Profile should show the Destination, taken from the ISDN Call Profile).<br>*Main Menu→ Status→ DBM Interface Status*<br>or the B channel's Frame Relay Performance Statistics screen.<br>*Main Menu→ Status→ Performance Statistics→ BRI-B1 Frame Relay*<br>Check Health and Status messages. You should not see **LMI Down** for the interface.<br>*Main Menu→ Status→ System and Test Status*<br>If you go to the unit's faceplate, the BKP (Backup) LED should not be lit because no data is being passed.<br>5. Return to Step 1, and disable the verified Destination.<br>6. Enable the next Destination to be tested, and repeat the procedure until all connections have been verified.<br>7. When all connections have been verified, re-enable all destination profiles. |

# Logins

Refer to Chapter 6, *Security and Logins*, to learn how to create and delete logins.

# Entering Identity Information

Use the Device Name screen to identify this system, and to change or display the general name, location, and contact for the system.

### ▶ Procedure

1. Follow this menu sequence:

   *Main Menu → Control → Device Name*

2. Place the cursor in the field (Tab to the field) where you want to add or change information.

   The following information is available for viewing. Use the right and left arrow keys to scroll additional text into view.

| If the selection is . . . | Enter the . . . |
|---|---|
| Device Name | Unique name for device identification of up to 20 characters. |
| System Name | SNMP system name; can be up to 255 characters. |
| System Location | FrameSaver access unit's physical location; can be up to 255 characters. |
| System Contact | Name and how to contact the system person; can be up to 255 characters. |

   **NOTE:**

   To clear existing information, place the cursor in the Clear field (Tab to the Clear field) and press Return.

3. To save changes, select Save and press Return.

   When Save is complete, Command Complete appears in the message area at the bottom of the screen.

# Configuring the FrameSaver Access Unit

Configuration option settings determine how the FrameSaver access unit operates. Use the access unit's Configuration menu to display or change configuration option settings.

## Configuration Option Areas

The FrameSaver access unit arrives with configured factory default settings, which are located in the Factory Default configuration option area. You can find the default settings for configuration options in the:

- *Quick Reference* included with the User's Guide
- Configuration option tables in this chapter
- Configuration worksheets in Appendix B

If the factory default settings do not support your network's configuration, you can customize the configuration options to better suit your application.

To change configuration option settings you must perform the following tasks:

- Access and display configuration option settings
- Change configuration option settings
- Save configurations option settings to a configuration option area

**NOTE:**

— Only Security Access Level 1 users can change configuration options.

— Security Access Level 2 users can only view configuration options and run tests.

— Security Access Level 3 users can only view configuration options; they cannot change configuration options or run tests.

The FrameSaver access unit offers four configuration option storage areas located in the following areas:

| Configuration Option Area | Description |
|---|---|
| Current Configuration | The access unit's set of currently active configuration options. |
| Customer Configuration 1 | The first of two alternate sets of configurations that can be set up by the customer and stored for future use. |
| Customer Configuration 2 | The second of two alternate sets of configurations that can be set up by the customer and stored for future use. |
| Default Factory Configuration | A read-only configuration area containing the factory default configuration options.<br>You can load and edit the default factory configuration settings, but you can only save those changes to the Current, Customer 1, and Customer 2 configuration option areas.<br>The Current, Customer 1, and Customer 2 configuration option areas are identical to the Default Factory Configuration until modified by the customer. |

## Accessing and Displaying Configuration Options

To access and display the configuration options, you must first load (copy) the applicable configuration option set into the edit area.

### ▶ Procedure

To load a configuration option set into the configuration edit area:

1. Follow this menu sequence:

   *Main Menu → Configuration*

2. The “Load Configuration From” screen appears. Select the configuration option area you want to load and press Return (Current Configuration, Customer Configuration 1, or Customer Configuration 2).

   The selected configuration option set is loaded into the configuration edit area and the Configuration Edit/Display screen appears.

## Changing Configuration Options

### ▶ Procedure

To change configuration option settings:

1. From the Configuration Edit/Display screen, select the configuration option set you want to view or make changes to and press Return.
2. Select the configuration options applicable to your network, and make appropriate changes to the setting(s).

   When creating new PVC connections or management PVCs, some configuration options will be blank. For a valid setting to appear, Tab to the configuration option and press the spacebar.

3. Repeat Steps 1 and 2 until all changes are complete.

## Saving Configuration Options

When all changes to the configuration options are complete, use the Save function key to save configuration option changes to either the Current, Customer 1, or Customer 2 Configuration areas.

### ▶ Procedure

To save the configuration options changes:

1. Press Ctrl-a to switch to the screen function key area.
2. Select the Save function key from any of the Configuration menu screens and press Return. The Save Configuration To screen appears.
3. Select the configuration option area where you want to save the changes to and press Return.

   When Save is complete, Command Complete appears in the message area at the bottom of the screen.

**NOTE:**

If you changed configuration options and try to exit the Configuration menu without saving those changes, a Save Configuration screen appears requiring a Yes or No response to saving the changes.

| If you select . . . | Then the . . . |
|---|---|
| No | Main Menu screen appears. Changes are not saved. |
| Yes | Save Configuration To screen appears. Choose a configuration option area to save to (e.g., Customer Configuration 1). |

**NOTE:**

There are other methods of changing configurations such as SNMP, DDS autobaud, and auto configuration. If the configuration that you have just loaded is changed via one of these other methods, then saving your configuration would cause the configuration change from the other method to be lost. A warning message is displayed if you attempt to save your configuration over a configuration changed by another method.

# Using Configuration Shortcuts

Configuration shortcuts allow you to force a set of configuration options that are appropriate to how the FrameSaver access unit will be configured or used. The access unit provides the following automatic configuration features:

- **Configuration templates** – To set up an application for the FrameSaver access unit during initial setup.

  Templates are for the most common applications of a FrameSaver access unit. When a template is selected, the DTE ports are enabled or disabled, Compression is enabled (if a compression template is selected), and the Port and Link Status configuration options are enabled. Then, only the appropriate sets of configuration options are visible for configuration.

- **Frame relay discovery** – To select a method of automatic configuration and connection of DLCIs within the FrameSaver access unit.

  When the network interface is configured as the user side of LMI (the most common configuration) and FR Discovery is selected, the FrameSaver access unit “discovers” network DLCIs from the network LMI status response message. Then, it configures network and port interface DLCIs, and automatically creates a PVC.

  Automatically-configured network DLCIs are multiplexed, and all automatically-configured port DLCIs carry the same DLCI Number as the network DLCIs. These are the same DLCI numbers that would have been available had the access unit not been inserted in the link between your equipment and the network.

The Configuration Template and FR Discovery features can be used in conjunction with or independent of one another (e.g., you can select a discovery mode without ever using a configuration template).

**NOTE:**

If using FR Discovery and the service provider does not use Annex D protocol, it is recommended that the network interface’s LMI Protocol be pre-configured along with the Node IP Address, Subnet Mask, and DS0 allocations before the deployment of remote FrameSaver access units. Otherwise, the feature will not work properly.

## Selecting a Configuration Template

Select Config Template to set up an application that reflects how the FrameSaver access unit will be used.

**NOTE:**

It is recommended that you do not change the application template used during initial setup. For example, if you used the 2Ports template when setting up, then select the 1Port template, the 1Port selection disables Port 2, although other settings configured for Port 2 remain unchanged.

### ▶ Procedure

To select an application template:

1. Follow this menu sequence:

   *Main Menu → Configuration Shortcuts → Config Template*

2. Select a template that indicates how the access unit will be used.

| Config Template | Application | Setup Configuration |
|---|---|---|
| 1Port | Only Port 1 will be used, and the data compression feature will not be used. | ■ Port-1 set to Enable, and Port-2 set to Disable.<br>■ Compression set to Disable.<br>■ Frame Relay Link Status set to Enable for both Port-1 and Network interfaces. |
| 1Port-Compr | Only Port 1 will be used, and the data compression feature will be used. | ■ Port-1 set to Enable, and Port-2 set to Disable.<br>■ Compression set to Enable.<br>■ Frame Relay Link Status set to Enable for both Port-1 and Network interfaces. |
| 2Ports | Both ports will be used, and the data compression feature will not be used. | ■ Both Port-1 and Port-2 set to Enable.<br>■ Compression set to Disable.<br>■ Frame Relay Link Status set to Enable for Port-1, Port-2, and Network interfaces. |
| 2Ports-Compr | Both ports will be used, and the data compression feature will be used. | ■ Both Port-1 and Port-2 set to Enable.<br>■ Compression set to Enable.<br>■ Frame Relay Link Status set to Enable for Port-1, Port-2, and Network interfaces. |
| None | No automatic configuration is used. | Configured manually by user (default). |

3. Save your selection.
4. Go to the Configuration menu and change the data rates for the Network and Port interfaces.
5. Change any node-specific configuration options that may be needed.

## Setting Up Automatic DLCI Configuration and Connection

Select FR Discovery for automatic configuration and cross-connection of DLCIs within the FrameSaver access unit. The FR Discovery mode defaults to 1MPort. When LMI is active on the network interface and the information on PVC status with provisioned DLCI numbers is next received from the Network service, the system will automatically save to the Current Configuration area the settings listed in the following table.

You can change the Frame Relay Discovery mode at any time, but no previously discovered and configured DLCIs or cross-connections are removed unless authorized. Additional discovered DLCIs will be configured according to the current Frame Relay Discovery mode. Selecting or changing a frame relay discovery method will not affect IP Addresses or Subnet Masks, either.

Configuration options set by a discovery mode can be manually modified, refined, or deleted via the Configuration menu.

**NOTE:**

Local Management PVCs (e.g., between a router and the FrameSaver access unit's data port) must be configured manually.

With 1MPort (Port 1 only, management DLCIs multiplexed with port DLCIs) as the default, a FrameSaver access unit can be sent to a remote site without preconfiguration other than the Node IP address, Subnet Mask, and LMI Protocol if Annex-D protocol is not used. The unit can be configured remotely through the management DLCI that is automatically "discovered" and created.

If 1MPort is not the setting required for your application, change the application template ***before*** connecting the network cable or editing the discovered configuration option settings. Otherwise, the FrameSaver access unit will start "discovering" DLCIs as soon as the unit powers up.

To recover from this problem if it occurs:

Select the desired FR Discovery mode, and Save. Save causes the **Delete All DLCIs and PVC Connections?** prompt to appear. Entering Yes clears all DLCI records and PVC connections, with exception to primary destination management PVCs configured on data ports. Not deleting management PVCs on the data port ensures that the connection between the local router and the unit remains operational.

**NOTE:**

If the unit at the other end of the network PVC is *not* a FrameSaver access unit, FR Discovery mode should be set to NetOnly, 1Port, or Disable; only one port can be used and no management DLCIs can be created.

In addition, PVC diagnostic tests cannot be run without disrupting data. This is because only FrameSaver models currently support port and PVC multiplexing, and PVC diagnostics.

**CAUTION:**

**Responding to the prompt with a Yes will delete manually configured or changed DLCIs and PVC connections, as well as the automatically configured ones.**

**Respond with a No if you have any manually configured DLCIs and PVC connections, or Alternate DLCIs or connections. Instead, delete selected DLCIs and PVC connections via the Configuration menu.**

## ▶ Procedure

To select a Frame Relay Discovery mode:

1. Follow this menu sequence:

   *Main Menu* → *Configuration Shortcuts* → *FR Discovery*

2. Select a Frame Relay Discovery mode.

| Select FR Discovery mode . . . | If the access unit's application will be . . . |
|---|---|
| 1Port | ■ Only Port-1 will be used.<br>■ Compression will not be enabled.<br>■ A multiplexed DLCI on the Network side will be created for Port-1 data.<br>■ No management DLCIs will be created. |
| 1MPort<br>*(default)* | ■ Only Port-1 will be used.<br>■ Compression will not be enabled.<br>■ A multiplexed DLCI on the Network side will be created for management and Port 1 data. |
| 1Port-Compr | ■ Only Port-1 will be used.<br>■ Compression will be enabled.<br>■ A multiplexed DLCI on the Network side will be created for Port-1 data.<br>■ No management DLCIs will be created. |
| 1MPort-Compr | ■ Only Port-1 will be used.<br>■ Compression will be enabled.<br>■ A multiplexed DLCI on the Network side will be created for management and Port 1 data.<br>■ DLCIs will be multiplexed. |

| Select FR Discovery mode . . . | If the access unit's application will be . . . |
|---|---|
| 2MPorts | ■ Both Port-1 and Port-2 will be used.<br>■ Compression will not be enabled.<br>■ DLCIs on the Network side will be created, each containing EDLCIs for Port-1 data, Port-2 data, and management traffic. |
| 2MPorts-Compr | ■ Both Port-1 and Port-2 will be used.<br>■ Compression will be enabled on Port 1.<br>■ DLCIs will be multiplexed. |
| NetOnly | ■ A multiplexed DLCI will be created on the Network side.<br>■ No port or management DLCIs, or PVC connections will be created. |
| Disable | ■ No port or management DLCIs, or PVC connections will be created.<br>■ No frame relay discovery takes place. Access unit will be configured manually. |

3. Save your selection.
4. Go to the Configuration menu and change any node-specific configuration options that may be needed.

The following table indicates the automatic configuration that occurs within the FrameSaver access unit when a frame relay discovery mode is selected.

**Automatic Configuration for Selected Frame Relay Discovery Mode (1 of 6)**

| If the mode selected is . . . | Then setup configuration is . . . |
|---|---|
| *No Management:*<br>■ 1Port<br>■ 1Port-Compr | ■ Network DLCI Records:<br>– DLCI Number is automatically created from the LMI status response message.<br>– DLCI Status is set to Active.<br>– DLCI Type is set to Multiplexed.<br>– CIR (bps) is automatically determined from LMI status update message if switch provides this information.<br>– Excess Burst Size (Bits) is calculated as the difference between the CIR and the port rate.<br>■ Port-1 Physical (1Port-Compr only):<br>– Compression is set to Enable.[1]<br>■ Port-1 DLCI Records:<br>– DLCI Number is automatically created from the network DLCI.<br>*Example:*<br>Network DLCI 1001 → Port-1 DLCI 1001<br>– DLCI Status is set to Active.<br>– CIR (bps) is automatically determined from the network.<br>– Compression is set to Enable for the first six DLCIs “discovered” (1Port-Compr only).<br>■ PVC Connections:<br>– Source Link is set to Port-1.<br>– Source DLCI is taken from the Port-1 DLCI Number.<br>– Primary Destination Link is set to Network.<br>– Primary Destination DLCI is taken from the network DLCI Number.<br>– Primary Destination EDLCI is 0.<br>■ Port-1 interface DLCI is automatically connected to the Network interface EDLCI within the access unit. |
| [1] When compression is enabled on Port-1, only the first 6 DLCIs configured will have Compression enabled, and no EDLCIs will be configured.<br>If Compression is manually disabled for one of the 6 DLCIs, the next new DLCI created will have Compression enabled. | |

**Automatic Configuration for Selected Frame Relay Discovery Mode (2 of 6)**

| If the mode selected is . . . | Then setup configuration is . . . |
|---|---|
| *Multiplexed Management:*<br>■ 1MPort<br>■ 1MPort-Compr | ■ Network DLCI Records:<br>– DLCI Number is automatically created from the LMI status response message. This DLCI will contain multiple EDLCIs: one for Port-1 and one for management.<br>– DLCI Status is set to Active.<br>– DLCI Type is set to Multiplexed.<br>– CIR (bps) is automatically determined from LMI status update message if switch provides this information.<br>– Excess Burst Size (Bits) is calculated as the difference between the CIR and the port rate.<br>■ Port-1 Physical (1MPort-Compr only):<br>– Compression is set to Enable.[1]<br>■ Port-1 DLCI Records:<br>– DLCI Number is automatically created for Port-1 from the multiplexed network DLCI.<br>*Example:*<br>Network DLCI 1001 →<br>Port-1 DLCI 1001<br>– DLCI Status is set to Active.<br>– CIR (bps) is automatically copied from the network.<br>– Compression is set to Enable for the first six DLCIs “discovered” (1MPort-Compr only). |

[1] When compression is enabled on Port-1, only the first 6 DLCIs configured will have Compression enabled, and no EDLCIs will be configured.

If Compression is manually disabled for one of the 6 DLCIs, the next new DLCI created will have Compression enabled.

**Automatic Configuration for Selected Frame Relay Discovery Mode (3 of 6)**

| If the mode selected is . . . | Then setup configuration is . . . |
|---|---|
| *Multiplexed Management: (cont'd)*<br>■ 1MPort<br>■ 1MPort-Compr<br>(cont'd) | ■ Management PVCs: [2]<br>– Name is automatically created from the network DLCI as Mgm*nnnn* (*nnnn* being the discovered multiplexed network DLCI number).[2]<br>*Example:*<br>Network DLCI 1001 → Port-1 DLCI 1001 and Mgm1001<br>– IP Address is taken from the Node IP Address.[2]<br>– Subnet Address is taken from the Node Subnet Address.[2]<br>– Primary (Destination) Link is set to Network.<br>– Primary (Destination) DLCI is automatically created from the network DLCI.<br>– Two Primary (Destination) EDLCIs are automatically created:<br>Port-1 data is always EDLCI 0.<br>Management data is always EDLCI 2.<br>– Set DE is set to Enable.<br>– RIP is set to Proprietary.<br>■ PVC Connections:<br>– Source Link is set to Port-1.<br>– Source DLCI is taken from the Port-1 DLCI Number.<br>– Source EDLCI is blank.<br>– Primary Destination Link is set to Network.<br>– Primary Destination DLCI is taken from the network DLCI Number.<br>– Two Primary Destination EDLCIs are automatically created:<br>Port-1 data is always EDLCI 0.<br>Management data is always EDLCI 2.<br>■ Port-1 interface and management DLCIs are automatically connected to the Network interface EDLCIs. |

[2] If the same DLCI/EDLCI combination already exists, no changes are made to the existing management PVC.

You may want to configure a unique Node IP Address and Subnet Mask, and create a management PVC for this address and subnet mask prior to FR Discovery.

**Automatic Configuration for Selected Frame Relay Discovery Mode (4 of 6)**

| If the mode selected is . . . | Then setup configuration is . . . |
|---|---|
| *Multiplexed Management: (cont'd)*<br>■ 2MPort*s*<br>■ 2MPorts-Compr | ■ Network DLCI Records:<br>– DLCI Number is automatically created from the LMI status response message. This DLCI will contain multiple EDLCIs: one for Port-1, one for Port-2, and one for management.<br>– DLCI Status is set to Active.<br>– DLCI Type is set to Multiplexed.<br>– CIR (bps) is automatically determined from LMI status update message if switch provides this information.<br>– Excess Burst Size (Bits) is calculated as the difference between the CIR and the port rate.<br>■ Port-1 and Port-2 DLCI Records:<br>– DLCI Number is automatically created for each port from the multiplexed network DLCI.<br>*Example:*<br>Network DLCI 1001 →<br>Port-1 DLCI 1001<br>Port-2 DLCI 1001<br>– DLCI Status is set to Active.<br>– CIR (bps) is automatically copied from the network.<br>■ Port-1 DLCI Records only:<br>– Compression is set to Enable for the first six DLCIs "discovered"(2MPorts-Compr only).<br>■ Port-1 Physical (2MPorts-Compr only):<br>– Compression on Port-1 is set to Enable.[1] |

[1] When compression is enabled on Port-1, only the first 6 DLCIs configured will have Compression enabled, and no EDLCIs will be configured.

If Compression is manually disabled for one of the 6 DLCIs, the next new DLCI created will have Compression enabled.

**Automatic Configuration for Selected Frame Relay Discovery Mode (5 of 6)**

| If the mode selected is . . . | Then setup configuration is . . . |
|---|---|
| *Multiplexed Management: (cont'd)*<br>■ 2MPorts<br>■ 2MPorts-Compr<br>(cont'd) | ■ Management PVCs: [2]<br>– Name is automatically created from the network DLCI as Mgm*nnnn* (*nnnn* being the discovered multiplexed network DLCI number).[2]<br>*Example:*<br>Network DLCI 1001 →<br>Port-1 DLCI 1001 and<br>Port-2 DLCI 1001 and<br>Mgm1001<br>– IP Address is taken from the Node IP Address.[2]<br>– Subnet Address is taken from the Node Subnet Address.[2]<br>– Primary (Destination) Link is set to Network.<br>– Primary (Destination) DLCI is automatically created from the network DLCI.<br>– Three Primary (Destination) EDLCIs are automatically created:<br>Port-1 data is always EDLCI 0.<br>Port-2 data is always EDLCI 1.<br>Management data is always EDLCI 2.<br>– Set DE set to Enable.<br>– RIP set to Proprietary.<br>■ PVC Connections:<br>– Source Link is set to Port-2.<br>– Source DLCI is taken from the Port-1 DLCI Number.<br>– Source EDLCI is blank.<br>– Primary Destination Link is set to Network.<br>– Primary Destination DLCI is taken from the network DLCI Number.<br>– Three Primary Destination EDLCIs are automatically created:<br>Port-1 data is always EDLCI 0.<br>Port-2 data is always EDLCI 1.<br>Management data is always EDLCI 2.<br>■ Port-1 (and Port-2) interface and management DLCIs are automatically connected to the Network interface DLCI. |

[2] If the same DLCI/EDLCI combination already exists, no changes are made to the existing management PVC.

You may want to configure a unique Node IP Address and Subnet Mask, and create a management PVC for this address and subnet mask prior to FR Discovery.

**Automatic Configuration for Selected Frame Relay Discovery Mode (6 of 6)**

| If the mode selected is . . . | Then setup configuration is . . . |
|---|---|
| ■ NetOnly | ■ Network DLCI Records:<br>– DLCI Number is automatically created from the LMI status response message. This DLCI will contain multiple EDLCIs: one for Port-1 and one for management.<br>– DLCI Status is set to Active.<br>– DLCI Type is set to Multiplexed.<br>– CIR (bps) is automatically determined from LMI status update message if switch provides this information.<br>– Excess Burst Size (Bits) is calculated as the difference between the CIR and the port rate. |

# Configuring Physical Options for Each Interface

Configure the physical characteristics for the following interfaces:

- Data ports
- Network
- ISDN BRI DBM (if installed)

## Setting Up a Port Interface's Physical Options

Select Physical to display or change the physical characteristics of the enabled data ports connected to DTEs (see Table 4-1).

*Main Menu → Configuration → Ports → [Port-1/Port-2] column → Physical*

### ▶ Procedure

1. Follow this menu sequence:

   *Main Menu → Configuration → Ports*

2. The Ports screen appears. Select to enable/disable Port 1 and Port 2.

3. Select Physical to change or display the physical configuration options for the enabled data port. Both the local and remote FrameSaver access units are configured alike.

**Table 4-1. Port Options (1 of 3)**

| **Port -*n*** |
|---|
| Possible Settings: **Enable, Disable**<br>Default Setting: **Enable** |
| Determines whether the synchronous data port is being used and can be configured.<br>▪ Port options do not appear if the port is set to Disable.<br>**Enable** – The port is active, and can be used to transmit and receive data.<br>**Disable** – The port is not active. When disabled, port configuration options do not appear and control, data, and clock leads for the port are in the off state.<br>NOTE: When the port is disabled, the access unit aborts any active frame relay and physical port tests, including any DTE-initiated loopback tests. |
| **Port Type** |
| Possible Settings: **EIA-232, V.35**<br>Default Setting: **V.35** |
| Identifies the interface type used for the data port.<br>**EIA-232** – The port is an EIA-232E-compatible DCE. An EIA-232-compatible DTE can be directly connected to the FrameSaver access unit, and requires no adapter cable.<br>**V.35** – The port is a V.35-compatible DCE. A V.35-compatible DTE can be connected to the access unit port using the EIA-530A-to-V.35 adapter cable (MS34 socket-to-plug). |

**Table 4-1. Port Options (2 of 3)**

| **Port Rate (Kbps)** |
|---|
| Possible Settings: **4.8, 9.6, 14.4, 16.8, 19.2, 24, 28.8, 38.4, 48, 56,** and **64 kbps** for EIA232 ports, or **4.8, 9.6, 14.4, 16.8, 19.2, 24, 28.8, 38.4, 48, 56, 64, 128, 192,** and **256 kbps** for V.35 ports<br>Default Setting: **56** |
| Specifies the bit rate for the port in kilobits.<br>NOTES: – Changing settings for this configuration option causes the access unit to abort any active frame relay tests.<br>– When Compression is enabled and Flow Control is set to Clock (see Flow Control configuration option on page 4-30), the port rate specified here is the maximum clock rate allowed for the port.<br>– When Compression is disabled, port speeds greater than 64 kbps should only be used to help reduce latency in transaction-processing environments since the network interface is only 64 kbps. Higher speeds should only be used for bursty data.<br>**4.8 – 64 kbps** – Sets the EIA-232 port type's bit rate from 4.8 to 64 kbps.<br>**4.8 – 256 kbps** – Sets the V.35 port type's bit rate from 4.8 to 256 kbps. |
| **Transmit Clock Source** |
| Possible Settings: **Internal, External**<br>Default Setting: **Internal** |
| Determines whether the DTE's transmitted data is clocked internally by the DCE or externally by the DTE connected to the port.<br>NOTE: Changing settings for this configuration option causes the access unit to abort any physical port tests, including any DTE-initiated loopback tests.<br>**Internal** – The DCE clocks transmitted data, and uses the interchange circuit DB (ITU 114) – Transmit Signal Element Timing (TXC) (DCE source) for timing the incoming data.<br>**External** – The DTE externally provides the clock for the transmitted data, and uses the interchange circuit DA (ITU 113) – Transmit Signal Element Timing (XTXC) (DTE source) for timing the incoming data. Do not use with compression unless the DTE can phase lock XTXC to TXC. |
| **Invert Transmit Clock** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Determines whether the clock supplied by the DCE on interchange circuit DB (ITU 114) – Transmit Signal Element Timing (DCE Source) TXC is phase inverted with respect to interchange circuit BA (ITU 103) – Transmitted Data (TD).<br>**Enable** – Phase inverts the DCE's TXC clock. Use this setting when long cable lengths between the access unit and the DTE are causing data errors.<br>**Disable** – Does not phase invert the DCE's TXC clock. |

**Table 4-1. Port Options (3 of 3)**

| **Port (DTE) Initiated Loopbacks** |
|---|
| Possible Settings: **Local**, **Disable**<br>Default Setting: **Disable** |
| Allows a local external DTE Loopback to be started or stopped via the port's attached data terminal equipment using the port's interchange lead LL (ITU 141).<br><br>**Local** – The DTE attached to the port controls the local external DTE Loopback.<br><br>**Disable** – The DTE attached to the port cannot control the local external DTE Loopback. |
| **Control Leads Supported** |
| Possible Settings: **Force, DTR, RTS, Both**<br>Default Setting: **Both** |
| Determines which control leads are supported by the DTE. The control leads determine when valid data is sent from the DTE. If valid data is not sent, data received from the DTE is not forwarded.<br><br>**Force** – Interchange circuits from the DTE are not monitored. Data sent from the DTE is always forwarded. DTR and RTS will not be monitored, but will be forced on internally.<br><br>**DTR** – Monitors DTR to determine when valid data is sent from the DTE. When DTR is off, data sent from the DTE is ignored and is not forwarded. LSD and CTS are dropped in response.<br><br>**RTS** – Monitors RTS to determine when valid data is sent from the DTE. When RTS is off, data sent form the DTE is ignored and is not forwarded. CTS is dropped in response.<br><br>**Both** – Monitors both DTR and RTS to determine when the DTE sends valid data. If either is off, data sent from the DTE is ignored and is not forwarded. |

## Configuring Port 1 for Data Compression

Select Compression to display or change the compression configuration options for Port 1 (see Table 4-2).

### ▶ Procedure

To configure Port 1 for compression:

1. Verify that Port 1 is enabled (Enable is the factory default setting).

   *Main Menu→ Configuration→ Ports→ Port 1 column→ Physical→ Port Status→ Enable*

2. Configure Port 1 for data compression (Disable is the factory default setting).

   *Main Menu→ Configuration→ Ports→ Port 1 column→ Compression→ Compression→ Enable*

3. Determine whether the attached unit (DTE) is a frame relay device, and if not, make the appropriate changes from the factory default settings.

   — Compression

   — DTE Type

| **If the device . . .** | **Then compression is done . . .** |
|---|---|
| Supports frame relay | On a per-DLCI basis from the Port 1 DLCI Records screen.<br>*Main Menu→ Configuration→ Ports→ Port 1 column→ DLCI Records* |
| Does not support frame relay | Over a single DLCI from the DLCI Records screen.<br>*Main Menu→ Configuration→ Network→ DLCI Records* |

**Table 4-2. Port-1 Compression Options (1 of 2)**

| **Compression** |
|---|
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Determines whether or not the port performs data compression.<br>**Enable** – The port performs data compression on up to six DLCIs. See Table 4-6.<br>**Disable** – The port does not compress data. |
| **DTE Type** |
| Possible Settings: **Frame Relay, Bit Synchronous**<br>Default Setting: **Frame Relay** |
| Identifies the protocol used by the data terminal equipment.<br>■ DTE Type does not appear if Compression is set to Disable.<br>**Frame Relay** – The DTE supports frame relay protocol.<br>**Bit Synchronous** – The DTE supports a bit synchronous protocol (HDLC, SDLC, PPP). Bit Synchronous cannot be selected if more than one DLCI is defined for the port. |
| **Compression Ratio Alarm** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Generates an alarm message when the compression ratio falls below a configurable threshold for the compressed DLCIs on Port 1.<br>■ Compression Ratio Alarm does not appear if Compression is set to Disable.<br>**Enable** – Generates Compression Ratio Alarm.<br>**Disable** – Does not generate Compression Ratio Alarm. |
| **Connection Failure Alarm** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Generates an alarm message when the connection for data compression between a local and remote access unit fails or cannot be established for the compressed DLCIs on Port 1.<br>■ Connection Failure Alarm does not appear if Compression is set to Disable.<br>**Enable** – Does not generate a Connection Failure Alarm.<br>**Disable** – Generates the Connection Failure Alarm. |

**Table 4-2. Port-1 Compression Options (2 of 2)**

| **Flow Control** |
|---|
| Possible Settings: **Clock, CTS, None**<br>Default Setting: **Clock** |
| Controls the flow of data sent from the DTE to the access unit.<br>■ Flow Control does not appear if Compression is set to Disable.<br><br>**Clock** – Varies the clock rate to match the current compression ratio on interchange circuits (ITU 114), Transmit Signal Element Timing (DCE source), TXC, and DD (ITU 115). However, if the Transmit Clock configuration option is set to External, the DTE must match the ETXC rate to the TXC supplied by the access unit. This flow control method provides higher throughput and lower latency for the compression connection. This is the recommended method for flow control as long as the DTE can accept a varying clock.<br><br>**CTS** – Turns CTS off when buffer space is low and on when sufficient buffer space exists to prevent the DTE from sending more data than can be handled. The DTE should not send packets when CTS is turned off.<br><br>**None** – Does not control the flow of data. Continues to accept data from the DTE as long as there is adequate buffer space. Packets will be discarded when the buffer is full. This setting is not recommended and is only used if the DTE does not recognize or is not compatible with Flow Control. |
| **Short Packet Bypass** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Enable** |
| Avoids data compression of short data packets received from the DTE, so performance is improved when data traffic predominantly consists of packets shorter than 80 bytes.<br>■ Short Packet Bypass does not appear if Compression is set to Disable.<br><br>**Enable** – Does not compress short packets received from the DTE.<br><br>**Disable** – Compresses all packets received from the DTE, regardless of packet length. |
| **Optimize Based On** |
| Possible Settings: **Throughput, Latency**<br>Default Setting: **Throughput** |
| Specifies how operation is optimized, via increased throughput or via decreased latency. This setting affects compression for all DLCIs.<br><br>**Throughput** – Specifies increased throughput to maximize operation.<br><br>**Latency** – Specifies decreased latency to maximize operation. Select this setting when rapid response time is the primary criteria. |

## Setting Up the Network Interface's Physical Options

Select Physical to display or change the physical configuration options for the Network interface (see Table 4-3).

*Main Menu* → *Configuration* → *Network* → *Physical*

**Table 4-3. Network Physical Options (1 of 3)**

| **Operating Mode** |
|---|
| Possible Settings: **DDS**, **LADS**<br>Default Setting: **DDS** |
| Selects the access unit's operating mode based on how it will be used in the network.<br><br>**DDS** – Specifies that the access unit is connected to the DDS network for standard DDS operation. In this application, autobaud (automatic rate-detection) is activated each time the access unit is powered-up or reset. The operating rate is either 56 kbps or 64 kbps CC.<br><br>**LADS** – Specifies that the access unit is used in a LADS (local area data set) application (also referred to as limited distance modem, or LDM). In this application, the local and remote access units are directly connected to one another via a private 4-wire cable facility (two twisted-pair, metallic-continuity, crossover circuits). The operating rate is 64 kbps. |
| **DDS Line Rate (Kbps)** |
| Possible Settings: **56, 64CC, Autobaud**<br>Default Setting: **Autobaud** |
| Forces the line speed for the Digital Data Service (DDS) line. This is the rate at which data is transmitted over the DDS line.<br><br>Only change this setting from Autobaud if the line speed previously provisioned by the service provider has changed, or if the access unit becomes stuck in Autobaud mode.<br>■ DDS Line Rate (Kbps) does not appear if Operating Mode is set to LADS.<br><br>**56** – Configures or forces the DDS line rate/speed to 56 kbps. Select 56 if the access unit is not running at the right speed.<br><br>**64CC** – Configures or forces the DDS line rate/speed to 64 kbps Clear Channel (72 kbps on the line). Select 64CC if the access unit is not running at the right speed.<br><br>**Autobaud** – Automatically changes the access unit's operating rate to the actual operating line rate of 56 kbps or 64CC as soon as a valid DDS network signal is detected (automatic rate-detection). It may take up to 15 seconds for automatic rate-detection and adjustment to occur. |

**Table 4-3. Network Physical Options (2 of 3)**

| **LADS Timing** |
|---|
| Possible Settings: **Internal, Receive**<br>Default Setting: **Receive** |
| Determines the the access unit's timing source when it is used in a LADs application.<br>■ LADS Timing does not appear if Operating Mode is set to DDS.<br>**Internal** – Derives timing from the access unit's local clock. Use this setting for the LADS primary timing unit that establishes the timing for both interconnected units.<br>**Receive** – Derives timing from the line's receive signal, except when the unit is running diagnostic tests that force the received signal to be the same as the access unit's tranmitted signal. Use this setting for a LADS secondary timing unit.<br>NOTE: Only one of the interconnected access units should be set to Network. |
| **DSU Latching Loopback** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Enable** |
| Specifies whether the access unit responds to the DSU Latching Loopback sequence sent by the network as specified by TR62310. Until the network receives the loopback release sequence, the access unit remains in the loopback.<br>**Enable** – Responds to the DSU latching loopback commands as specified by TR62310.<br>**Disable** – Does not respond to the DSU loopback commands or terminates the latching loopback test, if active. Causes the access unit to abort any active network DSU latching loopback tests.<br>NOTE: Because the latching loopback code is a control sequence (as opposed to a bipolar violation sequence), user data may cause the access unit to activate the loopback test. Use the Disable setting to provide a means of stopping the latching loopback test when the network did not command the test. |
| **Cross Pair Detection Alarm** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Enable** |
| Specifies whether to generate an alarm when a crossed-pair condition is detected.<br>**Enable** – Generates an alarm when a crossed-pair condition is detected.<br>**Disable** – Does not generate an alarm when a crossed-pair condition is detected. |
| **No Signal Alarm** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Enable** |
| Specifies whether an alarm is generated when a no-signal condition is detected.<br>**Enable** – Generates an alarm when a no-signal condition is detected.<br>**Disable** – Does not generate an alarm when a no-signal condition is detected. |

**Table 4-3. Network Physical Options (3 of 3)**

| **Out of Service Alarm** |
|---|
| Possible Settings: **Enable, Disable**<br>Default Setting: **Enable** |
| Specifies whether an alarm is generated when an out-of-service condition is detected on the Network interface.<br>**Enable** – Generates an alarm when an out-of-service condition is detected.<br>**Disable** – Does not generate an alarm when an out-of-service condition is detected. |
| **Out of Frame Alarm** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Enable** |
| Specifies whether an alarm is generated when an out-of-frame condition is detected on the Network interface.<br>**Enable** – Generates an alarm when an out-of-service condition is detected on the Network interface.<br>**Disable** – Does not generate when an alarm when an out-of-service condition is detected on the Network interface. |
| **Excessive BPV Alarm** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Enable** |
| Specifies whether an alarm is generated when excessive BPVs are detected.<br>**Enable** – Generates an alarm when excessive BPVs are detected.<br>**Disable** – Does not generate an alarm when excessive BPVs are detected. |

## Setting Up the ISDN BRI DBM Interface's Physical Options

Select Physical to display or change the physical configuration options for the ISDN BRI DBM (see Table 4-4) once ISDN Call Profiles have been setup (see *Creating, Displaying, or Changing ISDN Call Profiles* in Chapter 5).

*Main Menu* → *Configuration* → *ISDN BRI DBM* → *Physical*

### ▶ Procedure

1. Follow this menu sequence:

   *Main Menu* → *Configuration* → *ISDN BRI DBM*

2. The ISDN BRI B Channel screen appears. Enable or disable ISDN BRI bearer channel 1 (BRI-B1).

3. Select Physical to change or display the physical configuration options for the enabled ISDN BRI bearer channel.

**Table 4-4. ISDN BRI DBM Options (1 of 2)**

| **BRI-B1** |
|---|
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Determines whether the ISDN BRI DBM Bearer channel 1 (B1) is active so it can initiate or answer backup calls on the ISDN network interface.<br>**Enable** – Activates the DBM's Bearer channel.<br>**Disable** – Deactivates the DBM's Bearer channel. All other ISDN BRI DBM Bearer channel configuration options do not appear when this setting has been selected. |
| **Originate or Answer** |
| Possible Settings: **Originate, Answer**<br>Default Setting: **Answer** |
| Specifies whether the access unit's DBM will originate or answer dial backup calls. The DBM at one end of the circuit must be configured to originate calls, while the other must be configured to answer calls.<br>**Originate** – Places dial backup calls; the recommended setting for a remote site DBM. The Auto Answer configuration option does not appear when this setting has been selected.<br>**Answer** – Answers dial backup calls; the recommended setting for a central site DBM. The Call Attempts Timeout (minutes) configuration option does not appear when this setting has been selected. |
| **Switch Type** |
| Possible Settings: **NI-1**<br>Default Setting: **NI-1** |
| Specifies the type of switch used by the ISDN service provider. This option is for informational purposes only. This switch type supports the new national standard that all switches should support NI-1.<br>**NI-1** – National ISDN-1 |

**Table 4-4. ISDN BRI DBM Options (2 of 2)**

| **BRI-B1 Service Profile ID (SPID)** |
|---|
| Possible Settings: **3 – 20 digits**<br>Default Setting: **Clear** |
| Specifies the SPID number assigned by the ISDN service provider for Bearer channel 1 (B1). SPID numbers are used by the switch to identify which ISDN services the DBM can access. All blanks is a valid setting.<br><br>**3 – 20 digits** – Where you enter a SPID number, or you can leave blanks. If a nondigit/ numeric is entered, an Invalid Character (*x*) message appears at the bottom of the screen. If fewer than three digits/numerics are entered, an **Invalid – SPID must be at least 3 digits** message appears at the bottom of the screen.<br><br>**Clear** – Clears the SPID field so it can be re-entered. |
| **BRI-B1 Phone Number** |
| Possible Settings: **7 digits**<br>Default Setting: **Clear** |
| Provides the telephone number associated with Bearer channel 1 (B1). All blanks is a valid setting.<br><br>**7 digits** – Where you enter the telephone number. If a nondigit/ numeric is entered, an Invalid Character (*x*) message appears at the bottom of the screen. If fewer than seven digits/numerics are entered, an **Invalid – Phone number must be 7 digits** message appears at the bottom of the screen.<br><br>**Clear** – Clears the phone number field so it can be re-entered. |
| **BRI-B1 Manual Link Profile** |
| Possible Settings: **ASCII text entry**<br>Default Setting: Initially blank; no default. |
| Specifies the 8-character ISDN Profile associated with the remote unit. Used when manually placing backup calls.<br>■ BRI-B1 Manual Link Profile only appears when the ISDN BRI DBM Bearer channel is enabled and Originate or Answer is set to Originate.<br><br>**ASCII text entry** – Adds to or changes the BRI-B1 Manual Link Profile (maximum 8 characters). |

# Configuring Frame Relay Options for Each Interface

Configure the frame relay configuration options for the following interfaces:

- Data ports
- Network
- ISDN BRI (if installed)

Select Frame Relay from one of the interface screens (Network, Ports, or BRI-B1) to display or change the Frame Relay configuration options for the selected interface. All interfaces/ports are configured in the same manner. Port 1 has been selected for this procedure.

## ▶ Procedure

To configure interfaces to connect with the frame relay service:

1. Configure Port 1 Frame Relay Options.

   *Main Menu→ Configuration→ Ports→ Port 1 column→ Frame Relay*

   The frame relay link is already configured to be in service (Link Status is set to Enable).

2. Determine whether CIR enforcement should be changed (see Table 4-5).

   The factory default settings:

   — Inbound CIR Enforcement Mode is None

   — Outbound CIR Enforcement Mode is Forced

3. Based upon the information supplied by the service provider about the local management interface (LMI) and assigned line conditions, set the rest of the Frame Relay configuration options (see Table 4-5).

4. Configure Port 2 Frame Relay Options, referring to Steps 2 and 3.

   *Main Menu→ Configuration→ Ports→ Port 2 column→ Frame Relay*

**Table 4-5. Frame Relay Options (1 of 5)**

| **Link Status** |
|---|
| Possible Settings: **Enable, Auto, Disable**<br>Default Setting for user data ports and network interface: **Enable**<br>Default Setting for BRI channels: **Auto** |
| Determines whether the frame relay link for the interface is in service or out of service.<br><br>**Enable** – Frame relay link is in service. It causes data packets to be transmitted/received on the interface, and the LMI will be active.<br>■ If a data port or Network is the interface, select Enable to activate the interface's frame relay link.<br>■ If an ISDN BRI DBM B channel is the interface, select Enable for manual backup or when testing the ISDN link. This setting causes the DBM to originate or answer a call based upon how it is configured (see the Originate or Answer configuration option in Table 4-4).<br>If configured to originate a call, the DBM dials the Called ID in the ISDN Call Profile for the B channel configured as the Alternate Destination Link. If the B channel is disabled or already busy, the Called ID associated with the alternate B channel is called. If configured to answer a call, the DBM waits for a call on the B channel configured as the Alternate Destination Link. This allows testing of a B channel link.<br><br>**Auto** – Frame relay link is in service, as conditions warrant. Select Auto for a B channel or for a port connected to an external device (e.g., a modem) when Auto Backup is desired (see the Auto Backup configuration option in Table 4-18). It causes data packets to be transmitted/received on the interface and the LMI to be active when there is a failure of the Primary Destination Link or DLCI.<br>■ If an ISDN BRI DBM B channel is the interface and the DBM is configured to originate a call, the DBM dials the calling ID contained in the Alternate Destination Profile (see PVC Connections Options, Table 4-7).<br>When the primary link is restored, the access unit disconnects the call, and data is switched back to the primary link.<br>■ If an ISDN BRI DBM B channel is the interface and the DBM is configured to answer a call, the DBM waits for a call.<br>■ If a data port connected to an external device is the interface, the external device originates and answers calls.<br><br>NOTE: When an ISDN BRI DBM is installed, the DBM becomes active whenever a Source DLCI or Primary Destination DLCI is configured on the link for an ISDN Call Profile.<br><br>**Disable** – Frame relay is not in service. Does not transmit or receive data packets on the interface; the LMI is inactive.<br>■ If an ISDN BRI DBM B channel is the interface, is configured to originate a call, and frame relay Link Status is disabled, the access unit terminates existing call(s). This can be used to manually disconnect the call.<br>■ If an ISDN BRI DBM B channel is the interface, is configured to answer a call, and the frame relay Link Status is disabled, the access unit terminates existing call(s) and will not answer future calls on the B channel.<br>■ If a data port connected to an external device is the interface, the external device terminates calls. |

**Table 4-5. Frame Relay Options (2 of 5)**

| **Inbound CIR Enforcement Mode** |
|---|
| Possible Settings: **Forced, Standard, Discard**<br>Default Setting: **Forced** |
| Monitors and enforces the CIR for the frames received (inbound) across the frame relay interface (also known as *traffic shaping*). Applies to all the DLCIs configured for the interface.<br><br>CAUTION: The frame relay network may discard frames that exceed the CIR.<br><br>**Forced** – Monitors inbound DLCIs for excessive CIR for statistics collection, but CIR is not enforced. All frames are sent.<br><br>**Standard** – Monitors inbound DLCIs for excessive CIR. Discards frames that are marked DE, exceed the CIR, and are over the excess burst size. Sets the DE bit on outbound frames that exceed the CIR and are over the excess burst size if the DE bit is not already set.<br><br>**Discard** – Monitors inbound DLCIs for excessive CIR. Discards frames that exceed the CIR and are over the excess burst size, regardless of the DE bit setting. |
| **Outbound CIR Enforcement Mode** |
| Possible Settings: **Forced, Standard, Buffered**<br>Default Setting: **Forced** |
| Monitors and enforces the CIR for the frames transmitted (outbound) from the frame relay interface (also known as *traffic shaping*). Applies to all the DLCIs configured for the interface.<br><br>CAUTION: The frame relay network may discard frames that exceed the CIR.<br><br>**Forced** – Monitors outbound DLCIs, but the CIR is not enforced. Sends all frames whether or not sending them causes the rate to exceed the CIR for the DLCI. Discards the frame if holding it causes buffer space to become exhausted.<br><br>**Standard** – If sending the next frame causes the rate for the DLCI to exceed the CIR, sends the frame with the DE bit set, as long as it is within the excess burst size. Discards the frame if it is over the excess burst size.<br><br>**Buffered** – If sending the next frame causes the rate to exceed the CIR for the DLCI, then the frame is sent with the DE bit set, as long as it is within the excess burst size. Holds the frame if it is over the excess burst size, until sending it will not cause the excess burst size to be exceeded. |
| **LMI Personality** |
| Possible Settings: **User Side, Network Side**, **None**<br>Default Setting: **User Side** (for Network interface and answering BRI B channel), or **Network Side** (for data ports and originating BRI B channel) |
| Configures the frame relay or LMI to assume the role of either the user side or network side of the UNI.<br><br>■ LMI Personality does not appear if compression is enabled and DTE Type is set to Bit Synchronous.<br><br>**User Side** – LMI performs the functions specified for the user side of the UNI. Factory default for the network interface and answering BRI B channel. Use this setting when the interface is connected to a network.<br><br>**Network Side** – LMI performs the functions specified for the network side of the UNI. Factory default for the data ports and originating BRI B channel. Use this setting when a user side device is connected to the interface.<br><br>**None** – LMI does not exist and is not expected. None is not available for Network. |

**Table 4-5. Frame Relay Options (3 of 5)**

| **LMI Protocol** |
|---|
| Possible Settings: **Standard, Annex-A, Annex-D**<br>Default Setting: **Annex-D** |
| Specifies whether the LMI is supported on the frame relay interface, and if supported, which protocol is used.<br>■ LMI Protocol does not appear if:<br>– LMI Personality for Port-1 or Port-2 is set to Network Side because LMI Protocol is discovered automatically.<br>– Compression is enabled and DTE Type is set to Bit Synchronous.<br>CAUTION: For the network interface, if Annex-D is not being used, LMI Protocol must be changed before any FR Discovery (automatic configuration) takes place. This option must be configured correctly for FR Discovery (automatic determination and configuration) to take place.<br>Before deployment of access units where Annex D is not used, it is recommended that LMI Protocol be pre-configured along with the Node IP Address, Subnet Mask, and DS0 allocations.<br>**Standard** – Supports Standard LMI on the frame relay interface.<br>**Annex-A** – Supports LMI as specified by Q.933, Annex A.<br>**Annex-D** – Supports LMI as specified by ANSI T1.617, Annex D. |
| **LMI Error Event (N2)** |
| Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 10**<br>Default Setting: **3** |
| Configures the N2 parameter which sets the number of errors that can occur on the LMI link before reporting an error. Applies to both the user and network sides of the UNI.<br>■ LMI Error Event (N2) does not appear if:<br>– LMI Personality is set to None.<br>– Compression is enabled and DTE Type is set to Bit Synchronous.<br>**1 – 10** – Specifies the number of errors that can occur on the LMI link (inclusive). |
| **LMI Clearing Event (N3)** |
| Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 10**<br>Default Setting: **1** |
| Configures the LMI-defined N3 parameter which sets the number of error-free messages that must be received before clearing an error event. Applies to both the user and network sides of the UNI.<br>■ LMI Clearing Event (N3) does not appear if:<br>– LMI Personality is set to None.<br>– Compression is enabled and DTE Type is set to Bit Synchronous.<br>**1 – 10** – Specifies the number of error-free messages that must be received (inclusive). |

**Table 4-5. Frame Relay Options (4 of 5)**

| |
|---|
| **LMI Status Enquiry (N1)** |
| Possible Settings: **1, 2, 3, 4, . . . 255**<br>Default Setting: **6** |
| Configures the LMI-defined N1 parameter which sets the number of status enquiry polling cycles that the user side of the LMI initiates before a full status enquiry is initiated. Applies only to the user side of the UNI.<br>■ LMI Status Enquiry (N1) does not appear if:<br>– LMI Personality is set to None.<br>– Compression is enabled and DTE Type is set to Bit Synchronous.<br>**1 – 255** – Specifies the number of status enquiry polling cycles that can be initiated (inclusive). |
| **LMI Heartbeat (T1)** |
| Possible Settings: **5, 10, 15, 20, 25, 30**<br>Default Setting: **10** |
| Configures the LMI-defined T1 parameter which sets the number of seconds between the initiation of status enquiry messages on the user side of the LMI. Applies only to the user side of the UNI.<br>■ LMI Heartbeat (T1) does not appear if:<br>– LMI Personality is set to User Side or None.<br>– Compression is enabled and DTE Type is set to Bit Synchronous.<br>**5 – 30** – Specifies the number of seconds between the initiation of status enquiry messages in increments of 5. |
| **LMI Inbound Heartbeat (T2)** |
| Possible Settings: **5, 10, 15, 20, 25, 30**<br>Default Setting: **15** |
| Configures the LMI-defined T2 parameter which sets the number of seconds between the receipt of status enquiry messages on the network side of the LMI. Applies only to the network side of the UNI.<br>■ LMI Inbound Heartbeat (T2) does not appear if:<br>– LMI Personality is set to User Side or None.<br>– Compression is enabled and DTE Type is set to Bit Synchronous.<br>**5 – 30** – Specifies the number of seconds between the receipt of status enquiry messages in increments of 5. |
| **LMI N4 Measurement Period (T3)** |
| Possible Settings: **5, 10, 15, 20, 25, 30**<br>Default Setting: **20** |
| Configures the LMI-defined T3 parameter which determines the maximum number of status enquiry messages received in LMI Inbound Heartbeat (T2) before declaring an LMI Errored Event, and the time interval (in seconds) that the Local Management Interface's network side uses. Applies only when LMI Type is set to Standard and LMI Personality is set to Network Side of the UNI.<br>■ LMI N4 Measurement Period (T3) does not appear if:<br>– LMI Personality is set to User Side or None.<br>– Compression is enabled and DTE Type is set to Bit Synchronous.<br>**5 – 30** – Specifies the interval of time in increments of 5. |

**Table 4-5. Frame Relay Options (5 of 5)**

| **LMI Link Status Change Alarm** |
|---|
| Possible Settings: **Enable, Disable**<br>Default Setting: **Enable** |
| Specifies whether an alarm message is generated if the LMI link goes down or out of service.<br>■ LMI Link Status Change Alarm does not appear if:<br>– LMI Personality is set to None.<br>– Compression is enabled and DTE Type is set to Bit Synchronous.<br>– The interface is an ISDN BRI DBM and the DBM is configured for Answer (see Table 4-4).<br>**Enable** – Generates an ASCII alarm message if the LMI goes down.<br>**Disable** – Does not generate an ASCII alarm message if the LMI goes down. |
| **DLCI Status Change Alarm** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Enable** |
| Generates a DLCI link status change alarm message if the network sends a message indicating a status change for a DLCI. The network reports the status as Active, Inactive, Created, or Deleted. Applies only to the user side of the UNI.<br>■ DLCI Status Change Alarm does not appear if LMI Personality is set to Network Side or None.<br>**Enable** – Generates an ASCII alarm message if the network reports a status change for a DLCI.<br>**Disable** – Does not generate an ASCII alarm message if the network reports a status change for a DLCI. |

# Configuring DLCI Records for Each Interface

If Frame Relay Discovery Mode is not used, it is necessary to create DLCI records for each interface. If you do use Frame Relay Discovery Mode, then it may only be necessary to create alternate (backup) DLCIs, and a management DLCI between the access unit and the router.

Configure the DLCI records for the following interfaces:

- Data ports
- Network
- ISDN BRI DBM (if installed)

DLCI records for all interfaces are created and configured in the same manner. Procedures for creating DLCI Records for the Network, Data Port, and BRI interfaces are shown in the following examples.

### ▶ Procedure

To create and configure DLCI records:

1. Select DLCI records for the network, port, or ISDN BRI B channel.

   *Main Menu→ Configuration→ [Network/Port-1/Port-2/BRI]→ DLCI Records*

2. Select New and press Return to create a new DLCI. (The cursor is already positioned in the function key area so there is no need to press Ctrl-a.)

   The Network DLCI Record Entry screen appears, ready for input. The DLCI Number field is blank, while the rest of the fields are filled with the default value settings.

   **NOTE:**

   If there are already 40 DLCIs defined for this FrameSaver access unit, the message **No more DLCIs allowed** appears.

3. Enter the network DLCI number supplied by the network provider.

4. Determine the DLCI type; that is, determine whether the DLCI will be multiplexed.

   If so, change DLCI Type to Multiplexed.

5. Change the CIR and/or Excess Burst Size, if necessary.

6. Set the priority.

7. To create additional DLCI records, press Esc to return to the previous DLCI Records screen.

   **Helpful Hint:**

   Once you create the first DLCI record, you can use the CopyFrom function to create additional records, assigning a unique number to each new DLCI record.

   *Example:*
   First DLCI numbered 16
   Second DLCI numbered 17

8. Create additional DLCI records for the interface by selecting New or the CopyFrom function, if needed, and pressing Return.

   **Helpful Hint:**

   It is possible that the same DLCI number is assigned to more than one port. A DLCI Records Configuration Worksheet is provided in Appendix B to help you keep track of DLCI assignments.

### ▶ Procedure

To create and configure a Port 1 DLCI record:

1. Select Port 1 DLCI records.

   *Main Menu→Configuration→Ports→Port 1 column→DLCI Records*

2. Create Port 1 DLCI records and EDLCIs following the same procedure described on page 4-42, Steps 2 through 7.

   *Example:*
   Port 1 – DLCIs 101 and 102

See Table 4-6 for DLCI configuration options.

#### Compression Notes:

Remember, if compression is enabled and the connected DTE supports frame relay, configure frame relay configuration options for each DLCI.

If the connected DTE does not support frame relay, create only one DLCI to carry compressed data.

| **If compression is set to . . . ,** | **DTE Type is set to . . . ,** | **and the connected DTE . . .** | **Then . . .** |
|---|---|---|---|
| Enable (Table 4-2) | Frame Relay (Table 4-2) | supports frame relay | Up to 6 DLCIs can be compressed on Port-1 (Table 4-6). |
| Enable (Table 4-2) | Bit Synchronous (Table 4-2) | does not support frame relay | Only 1 DLCI can be created on the port (Table 4-6). |

3. If using compression, change or verify compression configuration options for the data carried by this DLCI.

   — DLCI Compression

   — DLCI Compression Mode

   — DLCI Compression Ratio Threshold

**Table 4-6. DLCI Records Options (1 of 2)**

| **DLCI Number** |
|---|
| Possible Settings: **16 – 1007**<br>Default Setting: Initially blank; no default. |
| Specifies the number for the DLCI in the DLCI record. The parameter determines which DLCI record is used for transferring data on a particular frame relay interface. DLCI numbers range from 0 to 1023. However, the numbers 0 – 15 and 1008 – 1023 are reserved. Entry of an invalid number results in the error message **Value Out of Range (16 – 1007)**.<br>■ DLCI Number does not appear if the DLCI number is part of a connection or has not been created yet.<br>NOTES: – If a DLCI number is not entered, the DLCI record is not created.<br>– The DLCI number entered must be unique for the interface.<br>– Changing settings for this configuration option causes the access unit to abort any active frame relay tests.<br>**16 – 1007** – Specifies the DLCI number (inclusive). |
| **DLCI Status** |
| Possible Settings: **Active, Inactive**<br>Default Setting: **Active** |
| Configures the DLCI to transfer information over the frame relay interface.<br>**Active** – The DLCI is active and can be used for the transfer of information on the frame relay interface.<br>**Inactive** – The DLCI is inactive and cannot be used for the transfer of information on the frame relay interface. Discards any frames received on this DLCI.<br>NOTE: Setting this configuration option to Inactive causes the access unit to abort any active frame relay tests. |
| **DLCI Type** |
| Possible Settings: **Standard, Multiplexed**<br>Default Setting: **Standard** |
| Specifies whether the DLCI is standard or multiplexed.<br>■ DLCI Type does not appear if Compression is enabled and the DTE Type is set to Bit Synchronous.<br>**Standard** – Supports standard DLCIs as specified by the Frame Relay Standards.<br>**Multiplexed** – Enables multiplexing of multiple connections into a single DLCI. Allows a single PVC through the frame relay network to carry multiple DLCIs as long as these connections are between the same two endpoints (proprietary). Do not select Multiplexed unless there are FrameSaver access units at both ends of the connection. |
| **CIR (bps)** |
| Possible Settings: **0 – 64,000**<br>Default Setting: **64,000** |
| Determines the data rate for the DLCI that the network commits to accept and carry without discarding frames; the CIR in bits per second. Entry of an invalid rate causes the error message **Value Out of Range (0 – 64000)**.<br>**0 – 64,000 bps** – Sets the network CIR (inclusive). |

**Table 4-6. DLCI Records Options (2 of 2)**

| |
|---|
| **Excess Burst Size (Bits)** |
| Possible Settings: **0 – 999,999**<br>Default Setting: **0** |
| Specifies the maximum amount of data that the network will accept beyond the CIR without discarding frames in bits. Entry of an invalid size causes the error message **Value Out of Range (0 – 999999)**.<br><br>**0 – 999,999 bits** – Specifies the amount of data that will accepted before frames are discarded (inclusive). |
| **DLCI Priority** |
| Possible Settings: **Low, Medium, High**<br>Default Setting: **Medium** |
| Specifies the relative priority for the DLCI (also known as *quality of service*).<br><br>**Low** – Data configured for the DLCI has low priority.<br><br>**Medium** – Data configured for the DLCI has medium priority.<br><br>**High** – Data configured for the DLCI has high priority. |
| **DLCI Compression** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Specifies whether data on a selected DLCI is compressed, and identifies the DLCIs on Port 1 that should not be compressed.<br>■ DLCI Compression does not appear if Compression is disabled on Port-1 and DTE Type is set to Bit Synchronous (see Table 4-2).<br><br>**Enable** – Compresses and decompresses this DLCI's data. Up to six Port 1 DLCIs can be configured for compression.<br><br>**Disable** –Does not compress and decompress this DLCI's data. Data is treated as standard frame relay information. |
| **DLCI Compr Ratio Alarm Threshold** |
| Possible Settings: **1.0:1, 2.0:1, 3.0:1, 4.0:1**<br>Default Setting: **1.0:1** |
| Specifies the compression ratio alarm threshold for the selected DLCI. An alarm is triggered for this DLCI if the dynamically measured compression ratio falls below the ratio specified by this configuration option.<br><br>**1.0:1** – Sets a ratio threshold of 1.0-to-1.<br><br>**2.0:1** – Sets a ratio threshold of 2.0-to-1.<br><br>**3.0:1** – Sets a ratio threshold of 3.0-to-1.<br><br>**4.0:1** – Sets a ratio threshold of 4.0-to-1. |

# Configuring PVC Connections

Select PVC Connections to display or change the configuration options for the PVC connections (see Table 4-7). You can configure up to 80 PVC connections.

## ▶ Procedure

1. Follow this menu sequence:

   *Main Menu → Configuration → PVC Connections*

2. The PVC Configuration Table screen appears. Select New or Modify from the PVC Configuration Table screen to add or change PVC connections between a source DLCI (link) and destination DLCI (link) on a frame relay interface.

   Also, to add or change an alternate destination DLCI for backup when the primary link or destination DLCI is down and a backup link has been established.

3. When New is selected, the configuration option field is blank. Tab to the first configuration option and press the spacebar. The first valid selection appears in the field.

   **NOTE:**

   Management links are not created using this screen. Go to the Management PVC Entry screen:

   *Main Menu → Configuration → Management and Communication → Management PVCs*

Frame relay is a peer-level protocol. If backup is used, there is no particular significance to which DLCI is designated as the source or destination; it is a matter of user preference. However, if backup is used, the Primary Destination DLCI may have an alternate destination specified.

**Table 4-7. PVC Connections Options (1 of 4)**

| **Source Link** |
|---|
| Possible Settings: **Network, Port-1, Port-2, BRI-B1, Clear**<br>Default Setting: Initially blank; no default. |
| Specifies the frame relay interface that starts a PVC connection; the *from* end of a from-to link. The only valid settings for this configuration option are frame relay interfaces that have at least one DLCI or EDLCI defined which are not part of a PVC connection or management link. For example, if Port 2 has no DLCIs defined, Port 2 would not appear as a valid setting.<br>**Network** – Specifies the Network interface as the source link.<br>**Port-1** or **Port-2** – Specifies the port as the source link.<br>**BRI-B1** – Specifies the ISDN B channel 1 as the source link.<br>**Clear** – Clears the Source Link and Source DLCI settings, and suppresses Source EDLCI. |

**Table 4-7. PVC Connections Options (2 of 4)**

| **Source DLCI** |
|---|
| Possible Settings: **16 – 1007**<br>Default Setting: Initially blank; no default. |
| Specifies the source DLCI for a frame relay interface. The DLCI must be defined and cannot be part of a PVC connection or management link.<br>■ Source DLCI has no value if Source Link contains no value.<br>**16 – 1007** – Specifies the DLCI number (inclusive). |
| **Source EDLCI** |
| Possible Settings: **0 – 62**<br>Default Setting: Initially blank; no default. |
| Specifies the source Embedded Data Link Connection Identifier (EDLCI) for a frame relay interface when a multiplexed DLCI record is selected as one end of a connection.<br>■ Source EDLCI only appears if Source DLCI contains a multiplexed DLCI record number.<br>**0 – 62** – Specifies the EDLCI number (inclusive). |
| **Source Profile** |
| Possible Settings: ASCII text<br>Default Setting: Initially blank; no default. |
| Specifies the source ISDN profile associated with the remote unit. Those ISDN profile IDs that you defined using *Main Menu* → *Control* → *ISDN Call Profiles* will be available for selection. Profiles are identified by number.<br>■ This configuration option only appears when Source Destination Link is set to BRI and an ISDN Call Profile has been defined. |
| **Primary Destination Link** |
| Possible Settings: **Network, Port-1, Port-2, BRI-B1, Clear**<br>Default Setting: Initially blank; no default. |
| Specifies the frame relay interface used as the primary destination link; the *to* end of a from-to link. The only valid settings for this configuration option are frame relay interfaces that have at least one DLCI or EDLCI defined which are not part of a PVC connection or management link. For example, if Port 2 has no DLCIs defined, Port-2 would not appear as a valid setting.<br>**Network** – Specifies the network interface as the primary interface.<br>**Port-1** or **Port-2** – Specifies the port as the primary interface.<br>**BRI-B1** – Specifies the ISDN B channel 1 as the primary interface.<br>**Clear** – Clears the Primary Destination Link and Primary Destination DLCI settings, and suppresses Primary Destination EDLCI. |

**Table 4-7. PVC Connections Options (3 of 4)**

| **Primary Destination DLCI** |
|---|
| Possible Settings: **16 – 1007**<br>Default Setting: Initially blank; no default. |
| Specifies the primary destination DLCI for a frame relay interface. The DLCI must be defined and cannot be part of a PVC connection or management link.<br>■ Primary Destination DLCI has no value if Primary Destination Link contains no value.<br>**16 – 1007** – Specifies the DLCI number (inclusive). |
| **Primary Destination EDLCI** |
| Possible Settings: **0 – 62**<br>Default Setting: Initially blank; no default. |
| Specifies the primary destination Embedded Data Link Connection Identifier (EDLCI) for a frame relay interface when a multiplexed DLCI record is selected as one end of a connection.<br>■ Primary Destination EDLCI only appears if Source DLCI contains a multiplexed DLCI record number.<br>**0 – 62** – Specifies the EDLCI number (inclusive). |
| **Primary Destination Profile** |
| Possible Settings: ASCII text<br>Default Setting: Initially blank; no default. |
| Specifies the primary destination ISDN profile associated with the remote unit. Those ISDN profile IDs that you defined using *Main Menu → Control → ISDN Call Profiles* will be available for selection. Profiles are identified by number.<br>■ This configuration option only appears when Primary Destination Link is set to BRI and an ISDN Call Profile has been defined. |
| **Alternate Destination Link** |
| Possible Settings: **Network, Port-1, Port-2, BRI, Clear**<br>Default Setting: Initially blank; no default. |
| Specifies the frame relay interface used as the alternate destination link; the *to* end of a from-to link that is used for backup when the primary destination link or DLCI is out of service. The only valid settings for this configuration option are frame relay interfaces that have at least one DLCI or EDLCI defined which are not part of a PVC connection or management link. For example, if Port 2 has no DLCIs defined, Port-2 would not appear as a valid setting.<br>**Network** – Specifies the network interface as the primary interface.<br>**Port-1** or **Port-2** – Specifies the port as the primary interface.<br>**BRI** – Specifies the ISDN B channel as the destination interface for backup.<br>**Clear** – Clears the Alternate Destination Link and Alternate Destination DLCI settings, and suppresses Alternate Destination EDLCI. |

**Table 4-7. PVC Connections Options (4 of 4)**

| **Alternate Destination DLCI** |
|---|
| Possible Settings: **16 – 1007**<br>Default Setting: Initially blank; no default. |
| Specifies the alternate destination Data Link Connection Identifier (DLCI) for a frame relay interface used for backup. The DLCI must be defined and cannot be part of a PVC connection or management link.<br>■ Primary Destination DLCI has no value if Primary Destination Link contains no value.<br>**16 – 1007** – Specifies the DLCI number (inclusive). |
| **Alternate Destination EDLCI** |
| Possible Settings: **0 – 62**<br>Default Setting: Initially blank; no default. |
| Specifies the alternate destination Embedded Data Link Connection Identifier (EDLCI) for a frame relay interface when a multiplexed DLCI record is selected as one end of a backup connection.<br>■ Alternate Destination EDLCI only appears if Source DLCI contains a multiplexed DLCI record number.<br>**0 – 62** – Specifies the EDLCI number (inclusive). |
| **Alternate Destination Profile** |
| Possible Settings: ASCII text<br>Default Setting: Initially blank; no default. |
| Specifies the alternate destination ISDN profile associated with the remote unit. Those ISDN profile IDs that you defined using *Main Menu → Control → ISDN Call Profiles* will be available for selection. Profiles are identified by number.<br>■ This configuration option only appears when Alternate Destination Link is set to BRI and an ISDN Call Profile has been defined. |

# Setting Test Timeout and Duration Options

Select General to display or change the general configuration options. Use the General Options screen (see Table 4-8). Follow this menu sequence:

*Main Menu* → *Configuration* → *General*

**Table 4-8. General Options**

| **Test Timeout** |
|---|
| Possible Settings: **Enable, Disable**<br>Default Setting: **Enable** |
| Determines whether or not user-initiated loopback and pattern tests have a duration after which they are terminated.<br><br>**Enable** – User-initiated Loopback and Pattern tests have a timeout. This setting is recommended when the access unit is managed remotely through an in-band data stream. If the access unit is accidently commanded to execute a test on the interface providing the management access, control can be regained after the timeout expires, terminating the test.<br><br>**Disable** – Loopback and pattern tests must be manually terminated. |
| **Test Duration (min)** |
| Possible Settings: **1 – 120**<br>Default Setting: **10** |
| Specifies the duration of the user-initiated loopback or pattern tests.<br>■ Test Duration (min) only appears if Test Timeout is set to Enable.<br><br>**1 – 120** – Sets the Test Timeout period in minutes (inclusive). |

# Configuring User Interface Options

Select User Interface to display or change the configuration options for the user interface. The User Interface Options menu contains the following selections:

- Communication Port
- External Device (COM Port)
- Telnet and FTP Sessions

## Setting Up the Communication Port

Select Communication Port to display or change the communication port configuration options (see Table 4-9). Follow this menu sequence:

*Main Menu* → *Configuration* → *User Interface* → *Communication Port*

**Table 4-9. Communication Port Options (1 of 4)**

| **Clock Source** |
|---|
| Possible Settings: **Internal, External**<br>Default Setting: **Internal** |
| Specifies whether the COM port uses internal or external clocking when set for synchronous operation. For synchronous operation, the COM port is always defined as a DCE. This configuration option reverses the direction of the clock (TXD, RXD) interchange circuits and allows the COM port to accept clocking from an external device.<br>■ Clock Source does not appear if Port Type is set to Asynchronous.<br>NOTE: Connection to another DCE requires a cross-over cable.<br>**Internal** – The COM port uses internal clocking.<br>**External** – The COM port uses external clocking. |
| **Port Use** |
| Possible Settings: **Terminal, Net Link, Alarm**<br>Default Setting: **Terminal** |
| Assigns a specific use to the COM port.<br>NOTES: – ASCII alarm messages may also be supported when the asynchronous terminal interface is not in use.<br>– If the Default Network Destination is set to COM (see Table 4-13) and you change Port Use to Terminal or Alarm, the Default Network Destination is forced to None.<br>**Terminal** – The COM port is the asynchronous terminal interface port.<br>**Net Link** – The COM port is the network communications link to the IP network or IP device port.<br>**Alarm** – The COM port is the ASCII alarm message port. This is an output only selection and cannot be used for the user interface.<br>CAUTIONS: If Net Link is used with an external modem attached to the COM port, be aware of the potential security risk of unwanted access to the NMS, or to other devices on the LAN to which the access device has routing table entries for subnet or host routes.<br>If you are to maintain a connection with the access unit, you need to have an alternate management path (Telnet through a PVC) configured ***before*** selecting Alarms and saving the configuration. |

**Table 4-9. Communication Port Options (2 of 4)**

| **Port Type** |
|---|
| Possible Settings: **Asynchronous, Synchronous**<br>Default Setting: **Asynchronous** |
| Specifies whether the port transmits synchronous or asynchronous data when it has been configured as the network communication link (Port Use set to Net Link). Asynchronous communication is assumed when Port Use is set to Terminal or Alarm.<br><br>**Asynchronous** – The port uses asynchronous communication.<br><br>**Synchronous** – The port uses synchronous communication. |
| **Data Rate (Kbps)** |
| Possible Settings: **9.6, 14.4, 19.2, 28.8, 38.4**<br>Default Setting: **19.2** |
| Specifies the rate for the COM port in kilobits per second.<br>■ Data Rate (Kbps) does not appear if Port Type is set to Synchronous and Clock is set to External.<br><br>**9.6** – Sets the COM port rate to 9600 bps.<br><br>**14.4** – Sets the COM port rate to 14,400 bps.<br><br>**19.2** – Sets the COM port rate to 19,200 bps.<br><br>**28.8** – Sets the COM port rate to 28,800 bps.<br><br>**38.4** – Sets the COM port rate to 38,400 bps. |
| **RIP** |
| Possible Settings: **None, Proprietary**<br>Default Setting: **None** |
| Specifies which Routing Information Protocol (RIP) is used to enable routing of management data between devices.<br><br>**None** – No routing is used. Use this configuration option when the device connected to the COM port is not a 9000 Series or 31*xx* Series device.<br><br>**Proprietary** – A proprietary variant of RIP version 1 is used to communicate routing information between devices to enable routing of IP traffic. Use this configuration option when the access unit is connected to another 9000 Series or 31*xx* Series device through the COM port. |
| **Character Length** |
| Possible Settings: **7, 8**<br>Default Setting: **8** |
| Specifies the number of bits needed to represent one character.<br>■ Character length defaults to 8 and cannot be changed if Port Use is set to Net Link and Port Type is set to Asynchronous.<br><br>**7** – Sets the character length to seven bits.<br><br>**8** – Sets the character length to eight bits. You must use this setting if using the COM port as the network communication link. |

**Table 4-9. Communication Port Options (3 of 4)**

| **Parity** |
|---|
| Possible Settings: **None, Even, Odd**<br>Default Setting: **None** |
| Provides a method of checking the accuracy of binary numbers for the COM port. A parity bit is added to the data to make the “1” bits of each character add up to either an odd or even number. Each character of transmitted data is approved as error-free if the “1” bits add up to an odd or even number as specified by this configuration option.<br><br>**None** – Provides no parity.<br><br>**Even** – Makes the sum of all 1 bits in the character and its corresponding parity bit always even.<br><br>**Odd** – Makes the sum of all 1 bits in the character and its corresponding parity bit always odd. |
| **Stop Bits** |
| Possible Settings: **1, 1.5, 2**<br>Default Setting: **1** |
| Determines the number of stop bits used for the COM port.<br><br>**1** – Provides one stop bit.<br><br>**1.5** – Provides one and a half stop bits.<br><br>**2** – Provides two stop bits. |
| **Ignore Control Leads** |
| Possible Settings: **Disable, DTR**<br>Default Setting: **Disable** |
| Specifies whether DTR is used.<br><br>**Disable** – Treats control leads as standard operation.<br><br>**DTR** – Ignores DTR. This may be necessary when connecting to some PAD devices. |
| **Login Required** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Determines whether a user ID and password (referred to as the login) is required in order to log on to the asynchronous terminal user interface connected to the COM port.<br>■ Login Required does not appear if Port Use is set to Net Link or Alarms.<br><br>**Enable** – Requires a login to access the user interface.<br><br>**Disable** – Does not requires a login. |

**Table 4-9. Communication Port Options (4 of 4)**

| **Port Access Level** |
|---|
| Possible Settings: **Level-1, Level-2, Level-3**<br>Default Setting: **Level-1** |
| Specifies level of user access privilege for the asynchronous terminal interface connected to the COM port.<br>■ Port Access Level does not appear if Port Use is set to Net Link or Alarms.<br>**Level-1** – Allows full access and control of the device including monitoring, diagnostics, and configuration. The user can add, change, and display configuration options, save, and perform device testing.<br>**Level-2** – Allows limited access and control of the device. The user can monitor and perform diagnostics, display status and configuration option information.<br>**Level-3** – Allows limited access with monitoring control only. The user can monitor and display status and configuration screens only. |
| **Inactivity Timeout** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Determines whether a user session is disconnected after a specified time of inactivity (no keyboard activity).<br>■ Inactivity Timeout does not appear if Port Use is set to Net Link or Alarms.<br>NOTE: Changing this setting does not affect the current session; it changes all subsequent sessions.<br>**Enable** – Disconnects user session after the specified time of inactivity.<br>**Disable** – Does not disconnect user session. |
| **Disconnect Time (Minutes)** |
| Possible Settings: **1 – 60**<br>Default Setting: **5** |
| Determines the amount of lapsed time before disconnecting a user session in minutes.<br>■ Disconnect Time (Minutes) does not appear if Port Use is set to Net Link or Alarms.<br>NOTE: Changing this setting does not affect the current session; it changes all subsequent sessions.<br>**1 – 60** – Sets the time from 1 to 60 minutes (inclusive). |

## Setting Up the COM Port to Support an External Device

Select External Device (Com Port) to display or change the configuration options that control call processing for an external device attached to the COM port (see Table 4-10).

*Main Menu* → *Configuration* → *User Interface* → *External Device (Com Port)*

**NOTE:**

To detect when the external device connection has been lost, the COM port's DTR lead should be connected to the external device's DSR lead using a standard EIA-232 crossover cable (the COM port's DTR lead is monitored for loss of connection). The external device must be configured to drop DSR when a disconnect occurs, and to ignore DTR.

**Table 4-10. External Device (COM Port) Options (1 of 2)**

| **External Device Commands** |
|---|
| Possible Settings: **Disable, AT, Other**<br>Default Setting: **Disable** |
| Specifies the type of commands to be sent over the COM port.<br>NOTE: The Carrier Detect (CD) lead detects loss of the external device, therefore the external device must not force CD on.<br>**Disable** – Commands will not be sent over the COM port.<br>**AT** – Standard Attention (AT) Commands are sent over the COM port to control the external device. All AT command strings will end with a carriage return (hex 0x0D) and a line feed (hex 0x0A).<br>**Other** – Commands configured by the user are sent out the COM port.<br>CAUTION: You must *not* use this setting if you have an async terminal connected to the COM port.<br>NOTE: Connect Prefix, Connect Indication String, Escape Sequence, Escape Sequence Delay, and Disconnect String options will only be used when the setting is Other. Refer to the Control Characters table on page 4-57. |
| **Dial-In Access** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Controls whether external devices can dial-in to the access unit through the COM port (based on the Communication Use option setting).<br>**Enable** – Answers incoming calls and establishes connection to the remote terminal or IP network.<br>**Disable** – Does not answer incoming calls. Refer to the Control Characters table on page 4-57. |

**Table 4-10. External Device (COM Port) Options (2 of 2)**

| |
|---|
| **Connect Prefix** |
| Possible Settings: **ASCII text entry, Clear**<br>Default Setting: **Clear** |
| Specifies the connect prefix to dial the directory phone number.<br><br>**ASCII text entry** – Adds to or changes the connect prefix (maximum 20 characters). Refer to the Control Characters table on page 4-57.<br><br>**Clear** – Clears the connect prefix. No connect prefix is used. Refer to the Control Characters table on page 4-57. |
| **Connect Indication String** |
| Possible Settings: **ASCII text entry, Clear**<br>Default Setting: **Clear** |
| Specifies the connect indication string that determines whether a connection is established. The access unit searches the COM port's receive data stream for the connect indication string. If not received within 1 minute, the connection times out.<br><br>**ASCII text entry** – Adds to or changes the connect indication string (maximum 20 characters). Refer to the Control Characters table on page 4-57.<br><br>**Clear** – Clears Connect Indication String. The COM port's receive data stream is not searched and the Carrier Detect (CD) lead is used to determine that a connection has been established. |
| **Escape Sequence** |
| Possible Settings: **ASCII text entry, Clear**<br>Default Setting: **Clear** |
| Specifies the COM port escape sequence used to switch an external device to command mode before the external device is commanded to disconnect.<br><br>**ASCII text entry** – Adds to or changes the escape sequence (maximum 20 characters).<br><br>**Clear** – Clears and sets the escape sequence. No escape sequence is sent out. |
| **Escape Sequence Delay (Sec)** |
| Possible Settings: **None, 0.2, 0.4, 0.6, 0.8, 1.0**<br>Default Setting: **None** |
| Specifies the delay before sending the first character of the escape sequence and the delay after the last character of the escape in seconds. During the delay, no data is sent from the COM port.<br><br>**None** – No COM port escape delay is used.<br><br>***x.x*** – The delay (0.2, 0.4, 0.6, 0.8, 1.0 seconds) used during the COM port's escape sequence. You must configure this delay for there to be a delay greater than or equal to the escape guard time, which is required by the external device. |
| **Disconnect String** |
| Possible Settings: **ASCII text entry, Clear**<br>Default Setting: **Clear** |
| Specifies the command used to disconnect an external device. Refer to the Control Characters table on page 4-57.<br><br>**ASCII text entry** – Adds to or changes the disconnect string (maximum 20 characters).<br><br>**Clear** – Clears Disconnect String. |

| Control Characters | | |
|---|---|---|
| **Sequence** | **ASCII** | **Hex** |
| ^A or ^a | SOH | 0x01 |
| ^B or ^b | STX | 0x02 |
| ^C or ^c | ETX | 0x03 |
| ^D or ^d | EOT | 0x04 |
| ^E or ^e | ENQ | 0x05 |
| ^F or ^f | ACK | 0x06 |
| ^G or ^g | BEL | 0x07 |
| ^H or ^h | BS | 0x08 |
| ^I or ^i | HT | 0x09 |
| ^J or ^j | LF or NL | 0x0A |
| ^K or ^k | VT | 0x0B |
| ^L or ^l | FF or NP | 0x0C |
| ^M or ^m | CR | 0x0D |
| ^N or ^n | SO | 0x0E |
| ^O or ^o | SI | 0x0F |
| ^P or ^p | DLE | 0x10 |
| ^Q or ^q | DC1 | 0x11 |
| ^R or ^r | DC2 | 0x12 |
| ^S or ^s | DC3 | 0x13 |
| ^T or ^t | DC4 | 0x14 |
| ^U or ^u | NAK | 0x15 |
| ^V or ^v | SYN | 0x16 |
| ^W or ^w | ETB | 0x17 |
| ^X or ^x | CAN | 0x18 |
| ^Y or ^y | EM | 0x19 |
| ^Z or ^z | SUB | 0x1A |
| ^{ or ^[ | ESC | 0x1B |
| ^\ or ^\| | FS | 0x1C |
| ^] or ^} | GS | 0x1D |
| ^^ or ^~ | RS | 0x1E |
| ^_ | US | 0x1F |

## Setting Up to Support a Telnet and/or FTP Session

Select Telnet and FTP Session to enable or disable a Telnet or download session. Telnet configuration options control whether a Telnet session is allowed through an interconnected IP network and the access security applicable to the session (see Table 4-11). Only one Telnet session can be active at any one time.

### ▶ Procedure

1. Set the Node IP Address, Node Subnet Mask, Default Network Destination (if it is the COM port or a management PVC has been specified), and the communication port's Link Protocol if the current setting is different from PPP (see Table 4-13). Follow this menu sequence:

   *Main Menu → Configuration → Management and Communication → Communication Protocol*

2. Specify the Primary DLCI number used for the management PVC for the frame relay interface (see Table 4-14). Follow this menu sequence:

   *Main Menu → Configuration → Management and Communication → Management PVCs*

3. Set the Telnet and FTP Sessions configuration options. Follow this menu sequence:

   *Main Menu → Configuration → User Interface → Telnet and FTP Sessions*

   The Telnet and FTP Session Options screen appears. The configuration options are in the following table (see Table 4-11).

4. Set the Port Use configuration option to Net Link (see Table 4-9). Follow this menu sequence:

   *Main Menu → Configuration → User Interface → Communication Port*

   This terminates the async terminal link and allows access via a Telnet or FTP session.

**Table 4-11. Telnet and FTP Session Options (1 of 2)**

| **Telnet Session** |
|---|
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Specifies whether the access unit will respond to a session request from a Telnet client on an interconnected IP network.<br><br>**Enable** – Allows Telnet sessions between the access unit and Telnet client.<br><br>**Disable** – Does not allow Telnet sessions. |
| **Telnet Login Required** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Specifies whether a user ID and password (referred to as the login) are required to access the user interface via a Telnet session. If required, the login used is the same login used for an async terminal interface session.<br><br>**Enable** – Requires a login to access a Telnet session.<br><br>**Disable** – Does not require a login. |
| **Session Access Level** |
| Possible Settings: **Level-1, Level-2, Level-3**<br>Default Setting: **Level-1** |
| Specifies the highest security level allowed when accessing the user interface via a Telnet session.<br><br>**Level-1** – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information, change configuration options, and run tests. This is the highest access level allowed. Use this setting when downloading files.<br><br>**Level-2** – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information and run tests only; they cannot change configuration options.<br><br>**Level-3** – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information only; they cannot change configuration options or run tests. |
| **Inactivity Timeout** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Determines whether a Telnet session is disconnected after a specified time of keyboard inactivity.<br><br>NOTE: Changing this setting does not affect the current session; it changes all subsequent sessions.<br><br>**Enable** – Terminates Telnet session after the specified time of inactivity.<br><br>**Disable** – Does not terminate Telnet session during inactivity. |

**Table 4-11. Telnet and FTP Session Options (2 of 2)**

| **Disconnect Time (Minutes)** |
|---|
| Possible Settings: **1 – 60**<br>Default Setting: **5** |
| Determines the amount of keyboard inactive time before disconnecting a user session.<br>■ Disconnect Time (Minutes) does not appear if Inactivity Timeout is set to Disable.<br>NOTE: Changing this setting does not affect the current session; it changes all subsequent sessions.<br>**1 – 60** – Sets the time from 1 to 60 minutes (inclusive). |
| **FTP Session** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Determines whether the access unit responds as a server when an FTP (file transfer protocol) client on an interconnected IP network requests an FTP session. Must be enabled when downloading files.<br>**Enable** – Allows an FTP session between the access unit and an FTP client.<br>**Disable** – Does not allow an FTP session. |
| **FTP Login Required** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Determines whether a user ID and password are required for an FTP session. If required, the login used is the same login used for an async terminal interface session.<br>**Enable** – User is prompted for a user ID and password.<br>**Disable** – User is not prompted for a user ID and password. |

# Configuring Alarms

Select Alarm from the Configuration Edit/Display menu to display or change the configuration options for the FrameSaver access unit's alarm and SNMP trap information (see Table 4-12). Alarm and SNMP trap configuration options control when and how alarm and trap conditions are automatically initiated by the access unit.

*Main Menu → Configuration → Alarm*

**Table 4-12. Alarm Options (1 of 2)**

| **ASCII Alarm Messages** |
|---|
| Possible Settings: **Com Port, Disable**<br>Default Setting: **Disable** |
| Controls the generation and routing of alarm messages to an ASCII terminal or printer attached to the COM port (either locally or remotely via an external device).<br><br>**Com Port** – Generates and sends ASCII alarm messages to the COM port when the Port Use option is set to Alarm (see Table 4-9, Communication Port Options).<br><br>**Disable** – Does not generate ASCII alarm messages. |
| **Alarm & Trap Dial-Out** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Controls whether alarm or SNMP trap messages initiate a call automatically when the COM port-connected external device establishes a connection with a remote modem. If the call cannot be completed and the Call Retry option is set to Enable, the alarm or SNMP trap message is held (queued) until the call completes, or until the maximum retry count is exceeded.<br><br>■ For alarms, if more that one alarm message is received while waiting for a call retry, only the highest priority alarm message is held; all previous messages are discarded.<br><br>■ For traps, when COM port is configured as a network communication link (Port Use set to Net Link), up to 10 SNMP trap messages are held at the COM port interface.<br><br>**Enable** – Automatically calls the phone number contained in the Control menu's COM Port Call Directories, Directory Number A (alarm).<br><br>**Disable** – For alarms, does not hold messages. For traps, where a COM port-connected external device has not completed the connection, holds the messages. |
| **Trap Disconnect** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Enable** |
| Determines whether the COM port-external device connection disconnects after the SNMP trap message has been sent. This configuration option only applies to external device connections initiated as a result of sending the SNMP trap message.<br><br>**Enable** – Disconnects the call after sending an SNMP trap message.<br><br>**Disable** – Does not disconnect the call and holds the line until it is disconnected manually or by the remote modem. This enables the NMS to poll the access unit for more information after receiving SNMP traps. |

**Table 4-12. Alarm Options (2 of 2)**

| **Call Retry** |
|---|
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Controls whether an incomplete call (busy, no answer, etc.) is retried when an alarm or SNMP trap message is sent to the COM port-connected external device.<br><br>**Enable** – Attempts to retry the call, up to 5 times per alarm or SNMP trap message, with a delay between each retry. The delay is specified by the Dial-Out Delay Time (Min) configuration option.<br><br>If an alternate dial-out directory is specified (see Alternate Dial-Out Directory), the alarm directory's telephone number is called first. If the call cannot be completed after 5 tries, then the alternate directory's telephone number is called (see the Control menu's COM Port Call Directories).<br><br>**Disable** – Does not retry an incomplete call. |
| **Dial-Out Delay TIme (Min)** |
| Possible Settings: **1 – 10**<br>Default Setting: **5** |
| Specifies the amount of time between call retries when an alarm or SNMP trap message is sent; the wait between call attempts (see Call Retry).<br><br>**1 – 10** – Sets the number of minutes for the delay between call retry attempts (inclusive). |
| **Alternate Dial-Out Directory** |
| Possible Settings: **None, 1 – 5**<br>Default Setting: **None** |
| Specifies whether an incomplete call (busy, or no answer, etc.) resulting from an attempt to send an alarm or SNMP trap message is retried using an alternate telephone number. Attempts the call up to 5 times per alarm or SNMP trap message. Up to 5 alternate call directories can be set up.<br><br>When Call Retry on Alarm or Trap is enabled, the alarm directory's telephone number is called first. If the call cannot be completed after 5 tries, then the specified alternate directory's telephone number is called.<br><br>**None** – Does not dial-out using one of the alternate directory telephone numbers.<br><br>**1 – 5** – Specifies the call directory containing the telephone number to call if a call cannot be completed using the telephone number in the alarm directory (Directory Number A in the Control menu's COM Port Call Directories), inclusive. |

# Configuring Management and Communication Options

Select Management and Communication to display the Management and Communications Options menu. The Management and Communication Options menu contains the following selections:

- Communication Protocol
- Management PVCs
- General SNMP Management
- SNMP NMS Security
- SNMP Traps
- Auto Backup Criteria

## Communication Protocol

Select Communication Protocol to display, add, or change the information necessary to support the IP communication network (see Table 4-13).

*Main Menu → Configuration → Management and Communication → Communication Protocol*

**Table 4-13. Communication Protocol Options (1 of 3)**

| **Node IP Address** |
|---|
| Possible Settings: **000.000.000.000 – 223.255.255.255, Clear**<br>Default Setting: **000.000.000.000** |
| Specifies the IP address needed to access the node. Since an IP address is not bound to a particular port, it can be used for remote access via a management PVC.<br><br>**000.000.000.000 – 223.255.255.255** – Shows the IP address for the node, which you can view or edit. The first digit (i.e., *nnn*.255.255.255) can be any number from 001 through 223, excluding 127. However, 000 is valid, representing a null address. Remaining digits (i.e., 255.*nnn.nnn.nnn*) can be any number from 000 through 255. Leading zeros are required.<br><br>**Clear** – Clears Node IP Address and fills the address with zeros (i.e., 000.000.000.000). |
| **Node Subnet Mask** |
| Possible Settings: **000.000.000.000 – 255.255.255.255, Clear**<br>Default Setting: **000.000.000.000** |
| Specifies the subnet mask needed to access the node. Since the subnet mask is not bound to a particular port, it can be used for remote access via a management PVC.<br><br>**000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the node, which you can view or edit.<br><br>**Clear** – Clears Node Subnet Mask and fills the address with zeros (i.e., 000.000.000.000). When the node's subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the class of the IP address: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000. |

**Table 4-13. Communication Protocol Options (2 of 3)**

| **Default Network Destination** |
|---|
| Possible Settings: **None, COM, *PVCname*** <br> Default Setting: **None** |
| Specifies where a default network destination or route is connected so that data without a specifically defined PVC will have a route. Examples: If the default network is connected to the communications port, you would select COM. If the default network is connected to a far-end device over the management PVC named Tpa (as defined by the Name configuration option (see Table 4-14), you would select the PVC name Tpa.<br><br>NOTE: If the link or network destination selected as the default route becomes disabled or down, the unrouteable data will be discarded. Make sure that the link selected is operational, and if that link goes down, change the default destination.<br><br>CAUTION: Use care when configuring a default route to an interface that has a subnet route configured at a remote end where the NMS, router, LAN adapter, terminal server, etc. is connected. Communicating with an unknown IP address on the subnet will cause temporary routing loops, which will last 16 iterations times the retry count.<br><br>**None** – No default network destination is specified. Unrouteable data will be discarded.<br><br>**COM** – Specifies that the default destination is connected to the COM port. Only appears when Port Use is set to Net Link (see Table 4-9).<br><br>***PVCname*** – Specifies a name for the management PVC. Only appears when a management PVC name is defined for the node For example, when the network is connected to a remote device located in Tampa, Tpa can be specified as the PVC name, which is the link between the local access unit and the one located in Tampa. Tpa would appear as one of the available selections. |
| ***COMMUNICATION (COM) PORT:*** |
| **IP Address** |
| Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** <br> Default Setting: **000.000.000.000** |
| Specifies the IP address needed to access the unit. Only in effect when the COM port is configured as a network communication link (Port Use option is set to Net Link, see Table 4-9).<br><br>**000.000.000.000 – 223.255.255.255** – Shows the IP address for the COM port, which you can view or edit. The first digit (i.e., *nnn*.255.255.255) can be any number from 001 through 223, excluding 127. Remaining digits (i.e., 255.*nnn.nnn.nnn*) can be any number from 000 through 255. Leading zeros are required.<br><br>**Clear** – Clears the IP address for the COM port and fills the address with zeros (i.e., 000.000.000.000). |

**Table 4-13. Communication Protocol Options (3 of 3)**

| **Subnet Mask** |
|---|
| Possible Settings: **000.000.000.000 – 255.255.255.255, Clear**<br>Default Setting: **000.000.000.000** |
| Specifies the subnet mask needed to access the unit. Only in effect when the COM port is configured as a network communication link (Port Use option is set to Net Link, see Table 4-9).<br><br>**000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the COM port, which you can view or edit.<br><br>**Clear** – Clears the subnet mask for the COM port and fills the address with zeros (i.e., 000.000.000.000). When the node subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the class of the IP address:<br>Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000. |
| **Link Protocol** |
| Possible Settings: **PPP, SLIP**<br>Default Setting: **PPP** |
| Specifies the link-layer protocol to be used. Only in effect when the COM port is configured as a network communication link (Port Use option is set to Net Link, see Table 4-9).<br><br>**PPP** – Point-to-Point Protocol.<br><br>**SLIP** – Serial-Line Internet Protocol. |
| **Alternate IP Address** |
| Possible Settings: **000.000.000.000 – 223.255.255.255, Clear**<br>Default Setting: **000.000.000.000** |
| Specifies the alternate IP address for the communication (COM) port. If this configuration option is not configured (i.e., it is zero), the COM port's primary IP address is used for the alternate telephone directory.<br><br>**000.000.000.000 – 223.255.255.255** – Shows the COM port's alternate IP address, which you can view or edit. The first digit (i.e., *nnn*.255.255.255) can be any number from 001 through 223, excluding 127. Remaining digits (i.e., 255.*nnn.nnn.nnn*) can be any number from 000 through 255. Leading zeros are required.<br><br>**Clear** – Clears the alternate IP address for the COM port and fills the address with zeros (i.e., 000.000.000.000). |
| **Alternate Subnet Mask** |
| Possible Settings: **000.000.000.000 – 255.255.255.255, Clear**<br>Default Setting: **000.000.000.000** |
| Specifies the alternate subnet mask needed to access the unit. Only in effect when the COM port is configured as a network communication link (Port Use option is set to Net Link, see Table 4-9).<br><br>**000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the COM port, which you can view or edit.<br><br>**Clear** – Clears the subnet mask for the COM port and fills the address with zeros (i.e., 000.000.000.000). When the node subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the class of the IP address:<br>Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000. |

## Setting Up Management PVCs

Select Management PVCs to define in-band management links by:

- Adding or changing Management PVCs for the FrameSaver access unit.
- Assigning the PVCs to the frame relay interface.

### ▶ Procedure

1. Follow this menu sequence:

   *Main Menu → Configuration → Management and Communication → Management PVCs*

2. Select New or Modify from the Management PVCs screen to add or change DLCI and EDLCI logical links. When you select New, the configuration option field is blank. When you select Modify, the values displayed for all fields are based on the PVC ID that you specified.

3. Tab to the configuration option and press the spacebar. The first valid selection appears in the field.

See Table 4-14 for Management PVCs configuration options.

**Table 4-14. Management PVCs Options (1 of 4)**

| **Name** |
|---|
| Possible Settings: **ASCII text entry**<br>Default Setting: Initially blank; no default. |
| Specifies a unique name for the management PVC as referenced on screens (e.g., Tpa for Tampa, Florida).<br><br>**ASCII text entry** – Where you enter a unique name for the management PVC (maximum length 4 characters). |
| ***Interface* IP Address** |
| Possible Settings: **Node-IP-Address, Special (000.000.000.000 – 223.255.255.255)**<br>Default Setting: **Node-IP-Address** |
| Specifies the IP address needed to access the unit via this management PVC, providing connectivity to an external IP network through the frame relay network.<br><br>**Node-IP-Address** – Uses the IP address contained in the Node IP Address configuration option (see Table 4-13, Communication Protocol Options).<br><br>**Special (000.000.000.000 – 223.255.255.255)** – Allows you to edit/display the IP address for the unit's management PVC when the IP address is different for this interface. The first digit (i.e., *nnn*.255.255.255) can be any number from 001 through 223, excluding 127. Remaining digits (i.e., 255.*nnn.nnn.nnn*) can be any number from 000 through 255. Leading zeros are required.<br><br>**Clear** – Clears the source/destination link and the DLCI field, and suppresses the source/destination EDLCI field. |

**Table 4-14. Management PVCs Options (2 of 4)**

| ***Interface* Subnet Mask** |
|---|
| Possible Settings: **Node-IP-Mask, Calculate, Special (000.000.000.000 – 255.255.255.255)**<br>Default Setting: **Node-IP-Mask** |
| Specifies the subnet mask needed to access the unit when the management PVC is providing connectivity to an external IP network (through frame relay) that requires a specific subnet mask for the interface.<br><br>**Node-IP-Mask** – Uses the *Interface* IP Subnet contained in the Node-Subnet Mask configuration option (see Table 4-13, Communication Protocol Options).<br><br>**Calculate** – Calculates the subnet mask created by the IP protocol based on the class of the IP address (Class A:255.000.000.000, Class B:255.255.000.000, or Class C: 255.255.255.000). Cannot be displayed or edited.<br><br>**Special (000.000.000.000 – 255.255.255.255)** – Allows you to edit/display the subnet mask for the management PVC when the subnet mask is different for this interface. A text field displays for you enter the subnet mask for this unit's management PVC. |
| **Primary Link** |
| Possible Settings: **Network, Port-1, Port-2, BRI-B1, Clear**<br>Default Setting: Initially blank; no default. |
| Specifies the primary frame relay interface to use for this management PVC. The interface selected must have at least one DLCI (or DLCI with EDLCI) defined, which is not part of a PVC connection or already assigned as a management PVC.<br><br>**Network** – Specifies the Network (NET) interface as the primary interface.<br><br>**Port-1** or **Port-2** – Specifies the port as the primary interface.<br><br>**BRI-B1** – Specifies the ISDN B channel 1 as the primary interface.<br><br>**Clear** – Clears the source/destination link and the DLCI field, and suppresses the source/destination EDLCI field.<br><br>NOTE: Clearing Primary Link also clears Primary DLCI. |
| **Primary DLCI** |
| Possible Settings: **16 – 1007**<br>Default Setting: Initially blank; no default. |
| Specifies the primary DLCI number used for the management PVC once the frame relay interface is selected.<br><br>The DLCI must be defined for the link (i.e., has a DLCI record), and it must not be part of a PVC connection or already assigned as a management PVC. For multiplexed DLCIs, at least one EDLCI must be unconfigured for the DLCI.<br><br>■ Primary DLCI is blank if the Primary Link field is blank.<br><br>NOTE: Clearing Primary Link also clears Primary DLCI.<br><br>**16 – 1007** – Specifies the DLCI number (inclusive). |

**Table 4-14. Management PVCs Options (3 of 4)**

| **Primary EDLCI** |
|---|
| Possible Settings: **0 – 62**<br>Default Setting: Initially blank; no default. |
| Specifies the EDLCI number used for a management PVC when a multiplexed DLCI is selected for the primary frame relay link. EDLCIs identify individual connections within multiplexed DLCIs that are unique to those DLCIs.<br><br>Use a unique EDLCI to identify an individual connection within a multiplexed DLCI. Use 0 to identify the primary EDLCI. Use 1 – 62 to identify secondary EDLCIs. Use the primary EDLCI for customer data, which has a higher utilization rate than management data, with slightly less line overhead.<br><br>■ Primary EDLCI does not appear if the Primary DLCI field does not contain a Primary DLCI that references a multiplexed DLCI.<br><br>NOTE: Clearing Primary DLCI or changing it to a standard DLCI clears Primary EDLCI.<br><br>**0 – 62** – Specifies the EDLCI number (inclusive). |
| **Primary Profile** |
| Possible Settings: ASCII text<br>Default Setting: Initially blank; no default. |
| Specifies the primary ISDN profile that is associated with the remote access unit. Those ISDN profile IDs that you defined using *Main Menu→ Control → ISDN Call Profiles* will be available for selection. Profiles are identified by number.<br><br>■ This configuration option only appears when Destination Link is set to BRI and an ISDN Call Profile has been defined. |
| **Alternate Link** |
| Possible Settings: **Network, Port-1, Port-2, BRI-B1, Clear**<br>Default Setting: Initially blank; no default. |
| Specifies the alternate frame relay interface to use for this management PVC. The interface selected must have at least one DLCI (or DLCI with EDLCI) defined, which is not part of a PVC connection or already assigned as a management PVC.<br><br>**Network** – Specifies the Network (NET) interface as the alternate interface.<br><br>**Port-1** or **Port-2** – Specifies the port as the alternate interface.<br><br>**BRI-B1** – Specifies the ISDN B channel 1 as the alternate interface.<br><br>**Clear** – Clears the source/destination link and the DLCI field, and suppresses the source/destination EDLCI field. |
| **Alternate DLCI** |
| Possible Settings: **16 – 1007**<br>Default Setting: Initially blank; no default. |
| Specifies the alternate DLCI number used for the management PVC once the frame relay interface is selected.<br><br>The DLCI must be defined for the link (i.e., has a DLCI record), and it must not be part of a PVC connection or already assigned as a management PVC. For multiplexed DLCIs, at least one EDLCI must be unconfigured for the DLCI.<br><br>■ Alternate DLCI is blank if the Alternate Link field is blank.<br><br>**16 – 1007** – Specifies the DLCI number (inclusive). |

**Table 4-14. Management PVCs Options (4 of 4)**

| **Alternate EDLCI** |
|---|
| Possible Settings: **0 – 62**<br>Default Setting: Initially blank; no default. |
| Specifies the EDLCI number used for a management PVC when a multiplexed DLCI is selected for the alternate frame relay link. EDLCIs identify individual connections within multiplexed DLCIs that are unique to those DLCIs.<br><br>Use a unique EDLCI to identify an individual connection within a multiplexed DLCI. Use 0 to identify the primary EDLCI. Use 1 – 62 to identify secondary EDLCIs. Use the primary EDLCI for customer data, which has a higher utilization rate than management data, with slightly less line overhead.<br><br>■ Alternate EDLCI does not appear if the Alternate DLCI field does not contain an Alternate DLCI that references a multiplexed DLCI.<br><br>**0 – 62** – Specifies the EDLCI number (inclusive). |
| **Alternate Profile** |
| Possible Settings: ASCII text<br>Default Setting: Initially blank; no default. |
| Specifies the alternate ISDN profile that is associated with the remote access unit. Those ISDN profile IDs that you defined using *Main Menu→ Control → ISDN Call Profiles* will be available for selection. Profiles are identified by number.<br><br>■ This configuration option only appears when Destination Link is set to BRI and an ISDN Call Profile has been defined. |
| **Set DE** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Specifies whether frames (packets) sent on a management PVC have the Discard Eligible (DE) bit set. This bit is used by the network to prioritize which frames to discard first during periods of network congestion. This allows management traffic to be viewed as lower priority than customer data.<br><br>**Enable** – Sets the DE bit to one on all frames sent on the management PVC.<br><br>**Disable** – Sets the DE bit to zero on all frames sent on the management PVC. |
| **RIP** |
| Possible Settings: **None, Proprietary**<br>Default Setting: **None** for a port interface**, Proprietary** for the network interface |
| Specifies which Routing Information Protocol (RIP) is used to enable routing of management between access units.<br><br>RIP default settings:<br><br>■ None if the Link field is a data port (Port *n*).<br>■ Proprietary if the Link field is set to Network.<br><br>**None** – Does not use routing protocol. Use this setting when the device at the other end of the management link is not a FrameSaver frame relay access unit. This is the factory default for management PVCs configured on user data ports.<br><br>**Proprietary** – Uses a proprietary variant of RIP version 1 to communicate routing information between FrameSaver frame relay access units. This is the factory default for management PVCs configured on the Network interface. |

## Setting Up for SNMP Management

Select General SNMP Management to add, change, or delete the information needed to allow the FrameSaver access unit to be managed as an SNMP agent by the NMS supporting the SNMP protocols.

*Main Menu → Configuration → Management and Communication → General SNMP Management*

See Table 4-15 for General SNMP Management configuration options.

**Table 4-15. General SNMP Management Options (1 of 2)**

| **SNMP Management** |
|---|
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Determines whether the access unit can be managed as an SNMP agent by an SNMP-compatible NMS.<br><br>**Enable** – Can be managed as an SNMP agent.<br><br>**Disable** – Cannot be managed as an SNMP agent. The access unit will not respond to SNMP messages nor send SNMP traps. |
| **Community Name 1** |
| Possible Settings: **ASCII text entry, Clear**<br>Default Setting: **Public** in ASCII text field |
| Specifies the first of two names that are allowed to access the objects in the access unit's MIB. The community name must be supplied by an external SNMP manager whenever the manager tries to access an object in the MIB.<br><br>**ASCII text entry** – Adds to or changes Community Name 1 (maximum 255 characters).<br><br>**Clear** – Clears Community Name 1. |
| **Name 1 Access** |
| Possible Settings: **Read, Read/Write**<br>Default Setting: **Read** |
| Specifies the type of access allowed to the objects in the MIB. This is the type of access allowed for external SNMP managers accessing MIB objects using Community Name 1.<br><br>**Read** – Allows read-only access (SNMP Get command). This includes all objects specified as either read-only or read/write in the MIB RFCs.<br><br>**Read/Write** – Allows read and write access (SNMP Get and Set commands). |
| **Community Name 2** |
| Possible Settings: **ASCII text entry, Clear**<br>Default Setting: **Clear** |
| Specifies the second of two names that are allowed to access the objects in the access unit's MIB. The community name must be supplied by an external SNMP manager whenever the manager tries to access an object in the MIB.<br><br>**ASCII text entry** – Adds to or changes Community Name 2 (maximum 255 characters).<br><br>**Clear** – Clears Community Name 2. |

**Table 4-15. General SNMP Management Options (2 of 2)**

| Name 2 Access |
|---|
| Possible Settings: **Read, Read/Write**<br>Default Setting: **Read** |
| Specifies the type of access allowed to the objects in the MIB. This is the type of access allowed for external SNMP managers accessing MIB objects using Community Name 2.<br><br>**Read** – Allows read-only access (SNMP Get command). This includes all objects specified as either read-only or read/write in the MIB RFCs.<br><br>**Read/Write** – Allows read and write access (SNMP Get and Set commands). |

## Setting Up for SNMP NMS Security

Select SNMP NMS Security to display, add, or change the SNMP security configuration options for the FrameSaver access unit. A table is displayed consisting of the network management systems identified by IP address that are allowed to access the access unit by SNMP.

*Main Menu → Configuration → Management and Communication → SNMP NMS Security*

See Table 4-16 for SNMP NMS Security configuration options.

**Table 4-16. SNMP NMS Security Options (1 of 2)**

| NMS IP Validation |
|---|
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Specifies whether security checks are performed on the IP address of SNMP management systems attempting to access the node. Allows access only if IP address of the sending manager is listed on the SNMP NMS Security Options screen.<br><br>**Enable** – Performs security checks.<br><br>**Disable** – Does not perform security checks. |
| **Number of Managers** |
| Possible Settings: **1 – 10**<br>Default Setting: **1** |
| Specifies the number of SNMP management systems that are authorized to send SNMP messages to the access unit. An IP address must be configured for each management system allowed to send messages. Configure IP addresses in the NMS *n* IP Address configuration option.<br><br>**1 – 10** – Specifies the number of authorized SNMP managers. |

**Table 4-16. SNMP NMS Security Options (2 of 2)**

| **NMS *n* IP Address** |
|---|
| Possible Settings: **000.000.000.000 – 223.255.255.255, Clear**<br>Default Setting: **000.000.000.000** |
| Specifies the IP address that identifies SNMP manager(s) authorized to send SNMP messages to the access unit. If an SNMP message is received from the NMS whose IP address does not match an address contained in this field, access is denied and an authenticationFailure trap is generated. If a match is found, the type of access (read-only or read/write) is determined by the corresponding access level.<br><br>**000.000.000.000 – 223.255.255.255** – Adds to or changes the NMS IP address. The first digit (i.e., *nnn*.255.255.255) can be any number from 001 through 223, excluding 127. Remaining digits (i.e., 255.*nnn.nnn.nnn*) can be any number from 000 through 255. Leading zeros are required.<br><br>**Clear** – Clears the NMS IP address and fills the address with zeros (i.e., 000.000.000.000). |
| **Access Type** |
| Possible Settings: **Read, Read/Write**<br>Default Setting: **Read** |
| Specifies the access allowed for an authorized NMS when IP address validation is performed. If the IP address for the NMS sending an SNMP message is on the list of allowed managers, this configuration option determines the type of access allowed for that manager.<br><br>**Read** – Allows read-only access (SNMP Get command) to the MIB objects. This includes all objects specified as either read-only or read/write in the MIB RFCs.<br><br>**Read/Write** – Allows read and write access (SNMP Get and Set commands) to the MIB objects. However, access for all read-only objects is specified as read-only. |

## Setting Up for SNMP Traps

Select SNMP Traps to display, add, or change the SNMP trap configuration options for the FrameSaver access unit.

*Main Menu → Configuration → Management and Communication → SNMP Traps*

To configure the FrameSaver access unit for SNMP traps you must set:

- The number of SNMP managers that are to receive SNMP traps from the FrameSaver access unit.
- An IP address for each SNMP manager specified.
- The type of SNMP traps to be sent from the FrameSaver access unit.

Use the SNMP Trap Options screen to configure the necessary configuration options needed to support the SNMP traps. Select and set the following configuration options, as appropriate (see Table 4-17).

**NOTE:**

Be sure to choose an operational link for the default. Should the default link become disabled, unrouteable traps will be discarded.

| **To . . .** | **Set the configuration option . . .** |
|---|---|
| Enable sending of SNMP trap messages | SNMP Traps to Enable. |
| Specify the number of SNMP managers that will receive SNMP trap messages from the access unit | Number of SNMP Managers to the desired number (maximum of 6) of SNMP managers to receive SNMP traps. |
| Specify an IP address for each SNMP manager specified in the Number of SNMP Managers configuration option | NMS *n* IP Address to the IP address that identifies each SNMP manager(s) indicated in the Number of SNMP Managers configuration option. |
| Specify the network destination for the Trap Manager | Destination to one of the following:<br>Default<br>COM<br>*PVCname* |
| Select the type of SNMP trap messages to be sent from the access unit | ■ General Traps to enable or disable warmStart and authenticationFailure traps.<br>■ Enterprise Specific Traps to enable or disable enterpriseSpecific traps.<br>■ Link Traps to enable or disable linkDown and linkUp traps.<br>■ DLCI Traps Interfaces to specify which interfaces will generate linkDown, linkUp and enterpriseSpecific traps. |

**Table 4-17. SNMP Traps Options (1 of 3)**

| **SNMP Traps** |
|---|
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Determines whether the access unit sends trap messages to the currently configured SNMP trap manager(s).<br><br>**Enable** – Sends trap messages.<br><br>**Disable** – Does not send trap messages. |
| **Number of Trap Managers** |
| Possible Settings: **1 – 6**<br>Default Setting: **1** |
| Specifies the number of SNMP management systems that will receive SNMP trap messages from the access unit. An NMS IP Address must be configured in the NMS *n* IP Address configuration option for each trap manager to receive trap messages.<br><br>**1 – 6** – Specifies the number of trap managers (inclusive). |
| **NMS *n* IP Address** |
| Possible Settings: **001.000.000.000 – 223.255.255.255, Clear**<br>Default Setting: Clear |
| Specifies the IP address that identifies the SNMP manager(s) to receive SNMP traps.<br>■ NMS *n* IP Address appears for each trap manager specified in the Number of Trap Managers configuration option.<br><br>**001.000.000.000 – 223.255.255.255** – Adds to or changes the IP address for the trap manager. The first digit (i.e., *nnn*.255.255.255) can be any number from 001 through 223, excluding 127. Remaining digits (i.e., 255.*nnn.nnn.nnn*) can be any number from 000 through 255. Leading zeros are required.<br><br>**Clear** – Clears the IP address and fills the address with zeros (i.e., 000.000.000.000). |
| **Destination** |
| Possible Settings: **Default, COM, *PVCname***<br>Default Setting: **Default** |
| Specifies the network destination for the Trap Manager number configuration option.<br>■ Destination appears for each trap manager specified in the Number of Trap Managers configuration option.<br><br>**Default** – Uses the default network.<br><br>**COM** – Uses the COM port. This selection only appears if the Communication Port Use configuration option is set to Net Link.<br><br>***PVCname*** – The management *PVCname* (name of the management PVC). This selection only appears when at least one management PVC is defined for the node. |

**Table 4-17. SNMP Traps Options (2 of 3)**

| **General Traps** |
|---|
| Possible Settings: **Disable, Warm, AuthFail, Both**<br>Default Setting: **Both** |
| Determines whether SNMP trap messages for warmStart and/or authenticationFailure events are sent to the currently configured trap manager(s).<br>**Disable** – Does not send trap messages for warmStart or authenticationFailure events.<br>**Warm** – Sends trap messages for warmStart events.<br>**AuthFail** – Sends trap messages for authenticationFailure events.<br>**Both** – Sends trap messages for both warmStart and authenticationFailure events. |
| **Enterprise Specific Traps** |
| Possible Settings: **Enable, Disable**<br>Default Setting: **Disable** |
| Determines whether trap messages for enterpriseSpecific events are sent to the currently configured trap manager(s).<br>**Enable** – Sends the following trap messages for enterpriseSpecific events.<br>Enterprise specific traps generated for the following events:<br>– enterpriseSelfTestFail(2) – Access unit hardware failure was detected during the access unit's self-test.<br>– enterpriseDeviceFail(3) – An internal device failures was detected by the access unit's operating software.<br>– enterpriseTestStart(5) – At least one test was started on an interface or virtual circuit.<br>– enterpriseTestStop(105) – All tests have stopped on an interface or virtual circuit.<br>– enterpriseConfigChange(6) – The configuration has been changed via the user interface or the NMS.<br>**Disable** – Does not send trap messages for enterpriseSpecific events. |
| **Link Traps** |
| Possible Settings: **Disable, Up, Down, Both**<br>Default Setting: **Both** |
| Determines whether SNMP linkDown or linkUp traps are sent to the currently configured trap manager(s). A linkDown trap indicates that the access unit recognizes a failure in one of the communication interfaces. A linkUp trap indicates that the access unit recognizes one of its communication interfaces is active.<br>Use the Link Traps Interface and the DLCI Traps on Interface configuration options to specify which interface will monitor linkUp and linkDown traps messages.<br>**Disable** – Does not send linkDown or linkUp trap messages.<br>**Up** – Sends trap messages for linkUp events.<br>**Down** – Sends trap messages for linkDown events.<br>**Both** – Sends trap messages for linkUp and linkDown events. |

**Table 4-17. SNMP Traps Options (3 of 3)**

| **Link Traps Interfaces** |
|---|
| Possible Settings: **Network, Ports, DBM, All**<br>Default Setting: **All** |
| Specifies which interface monitors and generates linkUp, linkDown, and enterpriseSpecific trap messages. These traps are not supported on the COM port.<br><br>**Network** – Generates trap messages for linkUp, linkDown, and enterpriseSpecific events on the DDS network interface.<br><br>**Ports** – Generates trap messages for linkUp, linkDown, and enterpriseSpecific events on the synchronous data ports.<br><br>**DBM** – Generates trap messages for linkUp, linkDown, and enterpriseSpecific events on the DBM only.<br><br>**All** – Generates trap messages for linkUp and enterpriseSpecific events on the DDS network interface and the synchronous data ports. |
| **DLCI Traps on Interfaces** |
| Possible Settings: **Network, Ports, DBM, All**<br>Default Setting: **All** |
| Specifies which interface will monitor and generate linkUp and linkDown trap messages for individual DLCIs. These traps are not supported on the COM port.<br><br>**Network** – Generates trap messages for linkUp and linkDown events on DLCIs for the network interface only.<br><br>**Ports** – Generates trap messages for linkUp and linkDown events on DLCIs for the synchronous data ports only.<br><br>**DBM** – Generates trap messages for linkUp and linkDown events on DLCIs for the DBM only.<br><br>**All** – Generates trap messages for linkUp and linkDown events on DLCIs for the DDS network interface and synchronous data ports. |

# Configuring Auto Backup

Select Auto Backup Criteria to change or display the configuration option that determines whether automatic backup is allowed.

*Main Menu → Configuration → Auto Backup Criteria*

See Table 4-18 for Auto Backup Criteria configuration options.

**Table 4-18. Auto Backup Criteria Options**

| **Auto Backup** |
|---|
| Possible Settings: **Enable, Disable,**<br>Default Setting: **Disable** |
| Determines whether backup for the access unit is automatically performed when the primary physical link or LMI, or a DLCI on a PVC connection fails.<br><br>When enabled, the access unit automatically enables the Alternate Link configuration option, and establishes an alternate DLCI and EDLCI, rerouting traffic over the backup interface. (See Table 4-14 to configure the alternate DLCI and alternate EDLCI.)<br><br>**Enable** – Reroutes traffic over the backup (alternate) interface.<br><br>**Disable** – Does not reroute traffic over the backup interface. |

## Restricting Auto Backup Based Upon the Time of Day

An NMS can provide time of day automatic backup control since the FrameSaver access unit does not have an internal time of day clock. The NMS switches configurations at the time of day automatic backup is allowed, then switches again during the hours when it is not allowed.

### ▶ Procedure

1. Configure for two sets of configuration options, specifying different destination circuits following this menu sequence:

   *Main Menu → Configuration → PVC Connections*

2. Store one configuration specifying only the primary destination circuit in the Customer Configuration 1 storage area.

   *PVC Connections → Save → Customer Configuration 1*

3. Store an alternate configuration specifying both the primary and alternate destination circuits in the Customer Configuration 2 storage area.

   *PVC Connections → Save → Customer Configuration 2*

4. Select a configuration from the NMS and save it.

| **If automatic backup is . . .** | **Then the NMS loads . . .** |
|---|---|
| Allowed | Customer Configuration 2:<br>*main/config/load → devConfigAreaCopy → customer2-to-active → main/config/save* |
| Not Allowed | Customer Configuration 1:<br>*main/config/load → devConfigAreaCopy → customer1-to-active → main/config/save* |

# Setting Up An ISDN BRI DBM

Before starting, obtain the following information:

- Verification that you have NI-1 ISDN service
- Verification of 1B+D service
- Verification of CNIS (calling number Identification service) for both the originating and answering units
- SPID (service profile identification)
- Actual phone number associated with the SPID
- Number of digits used for the Called ID or Calling ID (the ISDN Call Profile formats)

  *Example:*
  A 10-digit format with the area code included may be used for the Calling ID (8135309999), while a 7-digit format without the area may be used for the Called ID (5309999).

When configuring The FrameSaver access units with the ISDN BRI DBM option installed, remember that:

- If the one ISDN BRI DBM was configured to originate backup, the other ISDN BRI DBM must be configured to answer a backup call (see Table 4-4, the ISDN BRI DBM's physical options, page 4-34).
- If the one ISDN BRI DBM had been configured as the user side of LMI (LMI Personality), the other ISDN BRI DBM must be configured as the network side (see Table 4-5, the ISDN BRI DBM's frame relay options, page 4-37).

Print (or copy) the worksheets needed from Appendix B, and transfer this information to the appropriate configuration worksheets. Completing the following configuration worksheets before you start configuring the unit will speed setup time:

- ISDN BRI DBM Options Worksheet
- Frame Relay Options Worksheet
- DLCI Records Configuration Worksheet
- PVC Connection Table Configuration Worksheet

Begin setup of the ISDN BRI DBM, following the procedures in this section. Perform them in the order presented.

## Configure the ISDN BRI DBM Interface

### ▶ Procedure

1. Disable or verify that Auto Backup is disabled using the following menu-selection sequence:

   *Main Menu* → *Configuration* → *Auto Backup Criteria*

   **Helpful Hint:**

   Pressing the up arrow key (↑) with the cursor on the first menu selection moves the cursor to the last menu selection on the screen. Pressing the down arrow (↓) with the cursor on the last menu selection moves the cursor to the first menu selection.

2. Enable the ISDN BRI B channel:

   *Main Menu* → *Configuration* → *ISDN BRI DBM* → *Physical* → *BRI-B1*

   **Helpful Hint:**

   Available selections appear near the bottom of the screen, in the system messages and field values area under the function keys. (See screen example in Chapter 2 of the User's Guide, *Screen Work Areas*.)

3. Configure the ISDN BRI DBM interface's physical characteristics as indicated on the ISDN BRI DBM Options Worksheet:

   — Specify whether the DBM will Originate or Answer backup calls.

   — Enter the SPID and phone number for the enabled B channel.

   Saving your entries is not necessary at this point. Refer to Table 4-4, ISDN BRI DBM Options, page 4-32, for additional configuration information.

   **Helpful Hint:**

   Tab from field-to-field rather than pressing Enter to avoid clearing information just entered. Like the Enter key, the Tab key advances the cursor to the next field.

## Enter DLCI Records for the B Channel

### ▶ Procedure

1. Select DLCI Records for the ISDN BRI B channel:

   *Main Menu* → *Configuration* → *ISDN BRI DBM* → *DLCI Records*

2. Select New to create a DLCI record for the B channel. (The cursor is already in the function key area of the screen, so you do not have to press Ctrl-a.)

3. Enter the DLCI number indicated on the DLCI Records Configuration Worksheet to create the DLCI Records.

4. Press Ctrl-a to go to the function key area of the screen when finished creating DLCIs, and Save.

Refer to Table 4-6, DLCI Record Options, page 4-42, for configuration information.

## Set Up Frame Relay for the B Channel

### ▶ Procedure

1. Select BRI-B1 Frame Relay:

   *Main Menu* → *Configuration* → *ISDN BRI DBM* → *BRI-B1 Frame Relay*

   — Set the B channel's LMI Personality to either User Side or Network Side. (Remember, if the one ISDN BRI DBM is configured as the user side, the DBM at the other end must be configured as the network side.)

   — If configured to originate backup, enter the Manual Link Profile as indicated on the Frame Relay Options Worksheet.

   — Set the B channel's Link Status to Auto.

2. Modify other frame relay options, as indicated on the Frame Relay Options Worksheet.

Refer to Table 4-5, Frame Relay Options, page 4-37, for configuration information.

## Set Up the ISDN Call Profiles

### ▶ Procedure

1. Select ISDN Call Profiles:

   *Main Menu* → *Control* → *ISDN Call Profiles*

2. Set up the ISDN Call Profile(s). Up to three profiles can be set up.

   — Change Status to Enable.

   — Enter a name for the destination (e.g., Tampa). Up to 8 characters can be entered.

   — If the ISDN BRI DBM will be the originator, enter only the Called ID; the phone number for the DBM that will be called.

   If the ISDN BRI DBM will be answering the backup call, enter only the Calling ID for the DBM that will be calling.

3. Press Ctrl-a when finished setting up the profile(s), and Save.

   **CAUTION:**

   **You must Save Control menu changes before returning to the Main Menu or your entries will be lost.**

4. Reset the FrameSaver access unit to activate the SPID IDs:

   *Main Menu* → *Control* → *Reset Device*

   **Helpful Hint:**

   Remember to use the up arrow key (↑) to move the cursor to the last selection on the Control menu.

5. Enter Yes to the **Are you sure?** prompt (y and Enter). The FrameSaver access unit reinitializes itself.

See *Creating, Displaying, or Changing ISDN Call Profiles* in Chapter 5 for additional profile information; see *Resetting the FrameSaver Access Unit* for additional system reset information.

## Verify the ISDN Lines

Use either of the following methods to verify operation of the ISDN lines.

### ▶ Procedure

1. Check the status of the DBM interface:

   *Main Menu → Status → DBM Interface Status*

   Line Status should display Active. If an invalid (Inv) status appears (e.g., Inv SPID) in the Line Status field, verify that you entered the SPID, phone number, and Called or Calling ID in the ISDN Call Profile correctly.

2. Check the status of the FrameSaver access unit:

   *Main Menu → Status → System and Test Status → Health and Status column*

   **DSU Operational** should appear. If **ISDN Network Failed (Idle)** appears, check that both ends of the ISDN-U cable are seated properly for a good physical connection. If that does not clear the message, verify that you entered the SPID and phone number, and the ISDN Call Profile correctly.

See *DBM Interface Status* in Chapter 4 of the User's Guide for more DBM statuses, and *System and Test Status Messages* for more information on Health and Status messages.

**NOTE:**

Reset the FrameSaver access unit to activate the revised numbers after correcting a SPID.

## Modify the PVC Connection Being Backed Up

### ▶ Procedure

1. Follow this menu sequence:

   *Main Menu* → *Configuration* → *PVC Connections*

2. Press Ctrl-a to move the cursor to the function key area of the screen, and select Modify.

   The message **(Modify) or (Delete) Connection ID** appears.

3. Enter the ID number for the PVC to be backed up, and press Enter. The PVC Connection Entry screen for the selected PVC appears.

4. Add the following alternate destination (backup) information indicated on the PVC Connection Table Configuration Worksheet:

   — Set Alternate Destination Link to BRI.

   — Enter the Alternate Destination DLCI created for the B channel.

   — If there is a multiplexed DLCI, enter the Alternate Destination EDLCI created for the B channel.

   — Set Alternate Destination Profile to the ISDN Call Profile Destination

5. Press Ctrl-a, and Save.

## Set Up Automatic Backup

### ▶ Procedure

1. Follow this menu sequence:

   *Main Menu* → *Configuration* → *Auto Backup Criteria*

2. Enable Auto Backup.
3. Press Ctrl-a, and Save.

## Configure the Other End of the Circuit

Follow the same procedures to set up the ISDN BRI DBM in the FrameSaver access unit at the other end of the circuit, remember that:

- If the one ISDN BRI DBM was configured to originate backup, the other ISDN BRI DBM must be configured to answer a backup call (see Table 4-4, the ISDN BRI DBM's physical options, page 4-34).
- If the one ISDN BRI DBM had been configured as the user side of LMI (LMI Personality), the other ISDN BRI DBM must be configured as the network side (see Table 4-5, the ISDN BRI DBM's frame relay options, page 4-37).

## Verify the ISDN BRI DBM Setup

Once the ISDN BRI DBMs at both ends are set up, and their ISDN lines verified, you are ready to verify backup operation.

### ▶ Procedure

To monitor the backup operation:

1. View the status messages displayed at the bottom of the screen (lower right-hand corner, in the system messages and field values area),

   Or go to one of the following screens:

   — DBM Interface Status

   — System and Test Status, the Health and Status column

2. If viewing one of the status screens, select Refresh (r and Enter) to see the most current status.

### ▶ Procedure

To verify the backup operation:

1. Disconnect the network cable to monitor the results.
2. Check the status of the FrameSaver access unit:

   *Main Menu → Status → System and Test Status → Health and Status column*

3. Wait as the originating ISDN BRI DBM places the backup call.

   — Status messages change as the originating FrameSaver access unit calls the answering unit, and the originating unit's BKP LED starts blinking.

   — When the answering FrameSaver access unit receives the call, its BKP LED starts blinking, and the **ISDN Active** message appears.

   — The BKP LEDs of both units stop blinking and remain on when the connection is made, and the **Backup Active** message appears.

4. Verify that data is passing between the DBMs:

   *Main Menu → Status → Performance Statisitics → BRI-B1 Frame Relay*

5. Clear all statistics (c and Return).
6. Refresh the screen a few times:

   — Frames/Characters Sent and Frames/Characters Received (Frame Relay Link) increase when data is being passed.

   — Status Msg Received (Frame Relay LMI) also increases.

7. If the originating unit is dialing, but the answering unit is not receiving the call, recheck the SPIDs, phone numbers, and Calling and Called IDs at both units.
8. Reconnect the network cable to re-establish normal operation.

# Troubleshooting and Maintenance

# 5

## What Are the Troubleshooting and Maintenance Features?

The FrameSaver access unit can:

- Detect and report faults
- Perform diagnostic tests
- Download software
- Monitor statistics

Statistics are collected to help you determine how long a problem has existed.

These features ensure that your FrameSaver access unit is giving you optimum performance in your network.

## How Do I Know There Is a Problem?

The FrameSaver access unit offers a number of indicators to alert you to possible problems:

- LEDs
- Alarms
- SNMP Traps

If monitoring the system, the System and Test Status screen can also indicate that there is a problem.

*Main Menu → Status → System and Test Status*

# LEDs

The faceplate has twelve LEDs (Light Emitting Diodes) that provide status on the:

- Access unit
- Network interface
- DTE interface

Refer to *LEDs* in Chapter 5, *Maintenance and Troubleshooting*, of the User's Guide to interpret the LEDs.

You can view LED information on the following screens:

- Display LEDs
- Control

## Viewing Alarms and LEDs via the User Interface

View alarm and status change messages on the following async terminal interface screens:

- System and Test Status screen, using the following menu sequence:

  *Main Menu → Status → System and Test Status*

| **View . . .** | **To . . .** |
|---|---|
| Health and Status | Monitor the current status of the access unit.<br>Information appears in the order of its importance, highest priority to lowest. |
| Self-Test Results | Get the results of a power-up self-test or a reset of the access unit.<br>Includes a central processing unit (CPU) test, limited random access memory (RAM) test, and a device test on each card – the NAM and DBM, if installed. |
| Test Status | See which tests are currently active on this unit. |

- Display LEDs screen, using the following menu sequence:

  *Main Menu → Status → Display LEDs*

| **Select . . .** | **To . . .** |
|---|---|
| Display LEDs | Monitor the same conditions monitored by the front panel LEDs, using the user interface instead. |

### Selecting which Port's Status is Shown by the LEDs

Using the Control screen, you can assign which port's status appears on the front panel's LEDs. There are 12 LEDs on the FrameSaver access unit's faceplate. Refer to Chapter 5, *Maintenance and Troubleshooting,* of the *FrameSaver 9620 User's Guide* to understand what they indicate.

To view LED information via the user interface, see *Viewing Alarms and LEDs via the User Interface*, page 5-2.

#### ▶ Procedure

To select which port's status appears on the LEDs, follow this menu sequence:

*Main Menu → Control → Select LEDs → [Port-1/Port-2]*

The port change is immediate; the Save function is not required.

## Alarms

The FrameSaver access unit monitors alarm conditions occurring on the:

- Network interface
- Data ports
- Frame relay LMIs
- Frame relay DLCIs

### Viewing Alarm Messages

You can view alarm messages via the:

- Health and Status screen
- Messages on Line 24 of the user interface screen
- Printout from your ASCII terminal printer

Refer to Chapter 5, *Maintenance and Troubleshooting,* of the *FrameSaver 9620 User's Guide* for more information on alarms.

## Automatic Dialing Out When an Alarm Occurs

You can control whether generated alarm messages will initiate a call if a connection on the COM port external device has not already been established.

To dial out when an alarm occurs you must:

- Connect an external modem to the COM port.
- Select the ASCII alarms to receive for each interface.
- Set up the COM Port Call Directories.
- Enable Alarm & Trap Dial Out.
- Enable Call Retry, if desired.

### ▶ Procedure

To enable selected ASCII alarms for each interface:

1. Follow this menu sequence to display the Load Configuration From screen:

   *Main Menu* → *Configuration*

2. Select the desired configuration area and press Return. The Configuration Edit/Display screen appears.
3. Select the ASCII alarms to enable for the interface.

| **To enable . . .** | **Set the configuration option(s) . . .** |
|---|---|
| Network interface alarms | *Configuration* → *Network Interface* → *Physical* |
| Data Ports alarms | Configuration → Data Ports → Physical |
| Frame Relay DLCI alarms | Configuration → [*Interface*] → Frame Relay and Configuration → [*Interface*] → DLCI |

4. Configure the phone directory to use for dialing-out alarms (see *Displaying or Changing COM Port Directory Numbers* on page 5-8).
5. Select Alarm from the Configuration Edit/Display menu and press Return. The Alarms Options screen appears.

| **To . . .** | **Set the configuration option . . .** |
|---|---|
| Automatically initiate a call (dial out) | Alarm & Trap Dial-Out to Enable |
| Retry the call if the call cannot be completed | Call Retry to Enable |
| Enable ASCII alarms | Configuration → Alarm Options |

6. Press Ctrl-a to switch to the screen function key area.
7. To save changes, select Save and press Return. The Save Configuration To screen appears.
8. Select the configuration area where you want to save the changes to and press Return.

   When Save is complete, Command Complete appears at the bottom of the screen.

### Manual Dialing Out When an Alarm Occurs

Configure the external device connected the the FrameSaver access unit's COM port. Then, use the COM Port Call Setup screen to:

- Select the desired telephone number.
- Dial a call.
- Disconnect a call.

**▶ Procedure**

1. Follow this menu sequence:

   *Main Menu → Control → COM Port Call Setup*
2. Enter the desired directory number, or press the spacebar to cycle through the numbers that have been set up in the directory. The telephone number appears in the Directory Phone Number field.

   See *Maintaining COM Port Directories and ISDN Call Profiles* on page 5-7 for information about the call directory.
3. Select Dial and press the Enter key to initiate dialing.
4. To end the call, select Disconnect and press the Enter key.

## Supported SNMP Traps

The FrameSaver access unit supports the following traps:

- warm-start
- authentication-failure
- enterprise-specific (those specific to this access unit)
- link-up
- link-down

Refer to Appendix D for more information on traps.

## Selecting SNMP Traps

Select the SNMP traps you want to send using the following menu sequence:

*Main Menu → Configuration → Management and Communication → SNMP Traps*

The SNMP Trap Options screen appears.

## Dialing Out and Sending SNMP Traps

You can control whether generated SNMP trap messages will initiate a call if a connection on the COM port external device has not already been established. Use the Alarms Options screen to enable the FrameSaver access unit's automatic call initiation (dial out) on the COM port external device to send an SNMP trap message.

### ▶ Procedure

1. Assign SNMP Trap Managers. See *Setting Up for SNMP NMS Security* in Chapter 4, *Setting Up*.
2. Select the desired SNMP traps. See *Selecting SNMP Traps* on page 5-6.
3. Set up the COM Port Call Directories under the Control menu, and select a directory via the COM Port Call Setup screen.

   Set up the A directory as the primary alarm directory. You can also set up an alternate directory; refer to *Displaying or Changing COM Port Directory Numbers* on page 5-8.
4. Specify the IP address(es) of the NMS to send traps to when dialing out. Use the *Configuration → Management and Communication → SNMP NMS Security* menu sequence. See *Setting Up for SNMP NMS Security* in Chapter 4, *Setting Up*.
5. Enable the Call Retry and Alarm & Trap Dial-Out configuration options to hold the call if it cannot be completed. The call is held until completed, or the maximum retry count (maximum 5) has been exceeded. You can also set the delay time and specify an alternate directory, if desired.
6. Follow this menu sequence to display the Load Configuration From screen:

   *Main Menu → Configuration → [Current Configuration/ Customer Configuration 1/Customer Configuration 2]*
7. Follow this menu sequence to initiate a call:

   *Configuration Edit/Display → Alarm*

   The Alarm Options screen appears.

8. Select and set the following configuration options, as appropriate.

| To . . . | Set the configuration option . . . |
|---|---|
| Automatically initiate a call (dial out) | Alarm & Trap Dial-Out to Enable. |
| Retry the call if the call cannot be completed | Call Retry to Enable. |
| Specify whether to disconnect immediately after dialing out traps, or to allow a manual disconnect to occur. (A connection remains until manually disconnected.) | Trap Disconnect to Enable. |

9. Press Ctrl-a to switch to the screen function key area.
10. To save changes, select Save and press Return.
11. Select the configuration area where you want to save the changes to and press Return.

    When Save is complete, Command Complete appears at the bottom of the screen.

# Maintaining COM Port Directories and ISDN Call Profiles

Three Control menu selections are dedicated to dialing a remote device for management or providing backup via an external modem or internal ISDN BRI DBM:

| Select . . . | To . . . |
|---|---|
| COM Port Call Setup | Select a phone directory and view its phone number, or to initiate and terminate external modem connections over the access unit's COM port. Used for management. |
| COM Port Call Directories | Change the phone number contained in a selected directory when using an external modem. |
| ISDN Call Profiles | Enable the DBM's call profile, provide an identifier or name for the profile's destination, enter the phone number to call, and the Calling ID. Used for backup. |

## Displaying or Changing COM Port Directory Numbers

### ▶ Procedure

To display a COM port directory phone number, use the following menu sequence:

*Main Menu → Control → COM Port Call Setup*

### ▶ Procedure

To change a COM port directory phone number:

1. Use the following menu sequence:

   *Main Menu → Control → COM Port Call Directories*

2. To select the directory to be changed, press the number of the desired directory (1 through 5, or A for Alarm) and press Return. The phone number for that directory appears.
3. Review or change the phone number. Make sure only valid characters are entered when changing the phone number. Valid characters:
   - — Numbers 0 – 9
   - — Lowercase letters a – z
   - — Uppercase letters A – Z
   - — Space ( ) character
   - — ASCII symbols with the exception of the caret (^)
   - — Control sequence using the caret (^)
4. Press Ctrl-a to switch to the screen function key area.
5. To save changes, select Save and press Return.

   When Save is complete, Command Complete appears at the bottom of the screen.

**CAUTION:**

**Failure to save additions or changes to COM Port Call Directories will result in your entries being lost.**

## Creating, Displaying, or Changing ISDN Call Profiles

### ▶ Procedure

To create, display or change an ISDN call profile:

1. Use the following menu sequence to display or change directory phone numbers:

   *Main Menu → Control → ISDN Call Profile*

2. Select the number of the call profile to be created/displayed/changed, (up to 80 profiles, one per backup destination) in the ISDN Call Profile field. If a profile has already been created for the number that you entered, it appears on the screen. Otherwise, the fields are blank. Either the Called ID or the Calling ID (1,2) for the selected profile appears.

3. Enable or disable the selected call profile in the Status field.

4. Review or assign a name to this backup destination (usually the name of a site) in the Destination field.

5. Review or change the telephone number of the ISDN called or calling party identifier.

| **This field appears . . .** | **When the ISDN BRI DBM configuration option Originate or Answer is set to . . .** |
|---|---|
| Called ID | Originate |
| Calling ID (1 and 2) | Answer |

   Make sure only valid characters are entered when changing the phone number. Valid characters:

   — Numbers 0 – 9, *, #

   — Space ( ) or readability characters

   To ensure that the DBM installs the correct backup configuration upon answering, all calling party IDs must be unique across all of the enabled DBM call profiles. The FrameSaver access unit uses the Calling ID to identify the remote unit and to determine which PVC mappings to use.

6. To save changes, select Save and press Return.

**CAUTION:**

**Failure to save additions or changes to ISDN Call Profiles will result in your entries being lost.**

# Manual Dial Backup

Total manual control is provided for the times when automatic backup is not wanted. An alternate destination must have been configured for a backup call to take place.

Use these procedures to verify connections with data being passed. Refer to Step 18 of the *Recommended Order for Setup* in Chapter 4, *Setting Up*, to verify connections without data being passed – For an ISDN BRI DBM.

## ▶ Procedure

For total manual control when an alarm is received:

1. Configure for two sets of configuration options, specifying different destination circuits following this menu sequence:

   *Main Menu → Configuration → PVC Connections*

2. Store one configuration specifying only the primary destination circuit in the Customer Configuration 1 storage area.

   *PVC Connections → Save → Customer Configuration 1*

3. Store an alternate configuration specifying both the primary and alternate destination circuits in the Customer Configuration 2 storage area.

   *PVC Connections → Save → Customer Configuration 2*

4. When an alarm is received, manually load the desired configuration. For example:

   *Main Menu → Configuration → Load Configuration From → Customer Configuration 2*

5. Once the alarm is cleared, manually reload Customer Configuration 1.

## Forcing Backup Manually

Use this procedure to force backup when network maintenance is planned, when equipment problems are reported, or when testing the backup path – whenever data needs to be forced from the primary destination interface, typically the network, to the backup (alternate) interface or path.

Manual backup calls can be made via an:

- **External backup device** – For the devices at both ends of the PVC connection: Disable a primary destination network DLCI (which has an Alternate Destination DLCI configured) on the data port connected to the external backup device following this menu sequence:

  *Main Menu → Configuration → Network → [Port1/Port-2] → DLCI Records → DLCI Status → Inactive*

- **Internal ISDN BRI DBM** – With Auto Backup enabled, use one of three methods:

  — For the units at both ends of the PVC connection:

  Disable a primary destination network DLCI which has an Alternate Destination DLCI configured (on the ISDN B channel) following this menu sequence:

  *Main Menu → Configuration → Network → DLCI Records → DLCI Status → Inactive*

  — Disable frame relay Link Status on the network's Primary Destination channels following this menu sequence:

  *Main Menu → Configuration → Network → Frame Relay → Link Status → Disable*

  — Enable frame relay Link Status on the answering side of the ISDN B channel, then on the originating side, following this menu sequence:

  *Main Menu → Configuration → ISDN BRI DBM → Frame Relay → Link Status → Enable*

  Make sure the ISDN Call Profiles are correct and enabled.

  To determine the answering or originating side, see Originate or Answer in the DBM's physical options.

### ▶ Procedure

1. Configure the ISDN BRI DBM or external backup device's interface, including PVC connections, with an alternate destination specified.
2. Set up ISDN Call Profiles if using an ISDN BRI DBM, or the phone number in an external backup device.

| If using an . . . | Then select . . . |
|---|---|
| ISDN BRI DBM | ISDN Call Profiles:<br>*Main Menu → Control → ISDN Call Profiles*<br>■ ISDN Call Profile<br>■ Status<br>■ Destination<br>■ Called ID<br>■ Calling ID 1<br>■ Calling ID 2 |
| External backup device | Call Directories:<br>*Main Menu → Control → Call Setup*<br>■ Directory Number<br>■ Directory Phone Number |

3. Disable:
   - — The LMI for the Primary Destination Link – the frame relay Link Status configuration option, or
   - — The primary network DLCI(s) at both ends of the PVC connection in order to start dialing so the Alternate Destination DLCI(s) can be tested (see the DLCI Status configuration option in the DLCI Records Options, Table 4-6 of Chapter 4).
4. Verify that backup is taking place by viewing the:
   - — LMI Reported DLCIs screen of the backup port for LMI status.

     *Main Menu → Status → LMI Reported DLCIs → [Port1/Port-2/BRI-B1] → DLCI*
   - — PVC Connection Status screen for the DLCI's Alternate Destination.

     *Main Menu→ Status → PVC Connection Status*
   - — Health and Status messages; you should not see **LMI Down** for the port or B channel.

     *Main Menu→ Status→ System and Test Status*
   - — For the ISDN B channel, you can also view the DBM Interface Status.

     *Main Menu→ Status→ DBM Interface Status*

5. Verify that the faceplate's BKP (Backup) LED is lit; the unit is passing data. See Chapter 5, *Maintenance and Troubleshooting*, of the User's Guide if the LED does not light.
6. To discontinue the call once the backup path has been verified, re-activate the primary destination network DLCI at both ends of the PVC connection.

## Manual Backup When There Is a Failure

Use this procedure for total manually controlled backup when an alarm is received. An alternate destination has to have been configured for a backup call to take place.

### ▶ Procedure

1. Disable automatic backup.

   *Main Menu → Configuration → Auto Backup Criteria → Auto Backup → Disable*

2. Enable automatic backup when an alarm occurs, which indicates loss of:

   — Network link

   — LMI

   — DLCI

3. Verify that backup is taking place by viewing the:

   — LMI Reported DLCIs screen for the backup port.

   *Main Menu → Status → LMI Reported DLCIs → [Port1/Port-2] → DLCI*

   — PVC Connection Status screen for the DLCI's Alternate Destination.

   *Main Menu → PVC Connection Status*

4. Verify that the faceplate's BKP (Backup) LED is lit; the unit is passing data. See Chapter 5, *Maintenance and Troubleshooting*, of the User's Guide if the LED does not light.
5. To discontinue the call, disable automatic backup.

# Managing the FrameSaver Access Unit

Local management is accomplished through the following methods:

- DTE port configured with a frame relay management PVC, with the router providing RFC 1490 encapsulation of the IP traffic.
- COM port connected to an async terminal (or other VT100-compatible terminal) for direct access to the menu-driven user interface.
- COM port configured as an IP management link for Telnet access to the menu-driven user interface.
- COM port connected to the manager or router for an SNMP management link using UDP/IP and either PPP or SLIP as the link layer.
- COM port connected to an external LAN adapter for Ethernet or Token Ring connectivity for Telnet or SNMP management.

Remote management is accomplished via the following methods:

- Merging or multiplexing management data with user data, and transferring the information over a specified network PVC.
- Dedicated frame relay PVC between access units at each end of the circuit for in-band management.
- Management PVCs configured between DTE ports and RFC 1490-compliant routers at each end of the circuit to route management and user data through the same port to the routers.
- External modems connected to access unit COM port and the NMS for out-of-band management.
- Router connected to the access unit's COM port for out-of-band management.

Refer to Chapter 2, *Management Control and IP Addressing*, for additional information.

# Resetting the FrameSaver Access Unit

You can reset the FrameSaver access unit in four ways:

- Reset it from the Control menu to perform a self test
- Cycle the power to perform a self test
- Reset the configuration options to re-establish connectivity with the user interface
- Set the MIB from NMS

## Resetting the FrameSaver Access Unit from the Control Menu

Use this procedure to initiate a power-on selftest of the unit, recycling power.

### ▶ Procedure

To reset the FrameSaver access unit from the Control menu:

1. From the Main Menu screen, select Control and press Return. The Control menu appears.
2. Select Reset Device and press Return. The FrameSaver access unit reinitializes itself, performing a device self-test.

## Resetting the FrameSaver Access Unit via Power Recycling

Disconnecting, then reconnecting the power cord resets the access unit.

**NOTE:**

Make sure that the async terminal has Flow Control set to None for recycling to take place.

## Resetting the Access Unit's COM Port or Factory Defaults

Misconfiguring the FrameSaver access unit could render the user interface inaccessible, leaving it in a state where a session cannot be started via the COM port or a Telnet session. If this occurs, access unit connectivity can be restored via a directly-connected terminal.

Two methods can be used to restore access to the user interface:

- **Reset COM Port** – Allows you to reset the configuration options related to COM port usage. This also causes a device reset, where the FrameSaver access unit performs a Device Self-Test. No security-related configuration options are changed.
- **Reload Factory Defaults** – Allows you to reload the Default Factory Configuration, resetting all of the configuration and control settings which causes the current configuration to be destroyed and a device reset. This method is also useful when the user's password(s) have been forgotten.

### ▶ Procedure

To reset COM port settings:

1. At the async terminal that is directly connected to the FrameSaver access unit, configure the terminal to operate at 19.2 kbps, using character length of 8 bits, with one stop-bit, and no parity.

   In addition, set the async terminal's Flow Control to None.

2. Reset the FrameSaver access unit, then immediately and repeatedly press Return at a rate of about 1 press per second until the System Paused screen appears. (See *Resetting the FrameSaver Access Unit from the Control Menu* on page 5-15 to reset the unit.)

3. Tab to the desired method, and enter yes (or y) for the selected prompt.

| If entering yes to prompt . . . | Then . . . |
|---|---|
| Reset COM Port usage | ■ Port Type is set to Terminal.<br>■ Data Rate (kbps) is set to 19.2.<br>■ Character Length is set to 8.<br>■ Stop Bits is set to 1.<br>■ Parity is set to None.<br>■ External Device Commands is set to Disable. |
| Reload Factory Defaults | All factory-loaded configuration and control settings contained in the Default Factory Configuration configuration area are loaded. |

If no (or n) is entered, or if no selection is made within 30 seconds, the FrameSaver access unit returns to the condition or operation it was in when the system reset was initiated, with the COM port rate returning to its configured rate.

The access unit resets itself, going through a Device Self-Test. Connectivity is restored and the Main Menu screen appears.

## Resetting or Clearing Performance Statistics

You can clear all performance statistics, or clear statistics for a selected interface using the Clear Statistics menu. For DDS network physical statistics, only user statistics can be cleared. Telco statistics cannot be cleared.

**NOTE:**

You can also use the ClrStats function at the bottom of Performance Statistics screens to clear only the statistics shown on that screen.

— Compression statistics cannot be cleared from the NMS.

### ▶ Procedure

To clear performance statistics from the Clear Statistics menu:

1. Use the following menu sequence:

   *Main Menu* → *Status* → *Performance Statistics* → *Clear Statistics*

2. Select All or the interface (Network, Port-1, Port-2, or BRI) for which you want performance statistics cleared.

   If All is selected from the Clear Statistics menu, all interface statistics are cleared; no additional Clear Statistics menu for the selected interface appears.

   If an interface is selected, the statistics associated with that interface appear.

3. Select All or a specific set of statistics (Physical, Frame Relay Link, Frame Relay Error, Frame Relay LMI, or DLCI) for which you want performance statistics cleared.

   If All is selected from the Clear *Interface* Statistics menu, all statistics for the selected interface are cleared.

   If a specific set of statistics (statistics register) is selected, only the selected statistics register is cleared.

The following table explains the performance statistics that are cleared when you make selections.

| For interface . . . | Select . . . | To clear . . . |
|---|---|---|
| **Clear Statistics menu** | | |
| Network<br>Port-1,<br>Port-2,<br>BRI-B1 | All | All statistics for all interfaces (DDS network, both ports, and B channel statistics); no additional menu appears. |
| | Network | Statistics for the selected interface;<br>Clear *Interface* Statistics menu appears. |
| | Port-1 | |
| | Port-2 | |
| | BRI[1] | |
| **Clear *Interface* Statistics menu** | | |
| Network<br>Port-1,<br>Port-2,<br>BRI-B1 | All | All statistics for the selected interface (physical, frame relay link, frame relay error, frame relay LMI, or selected DLCI). |
| | Physical | Only statistics associated with the physical interface: DDS network (NET), port (Port 1 or Port 2), or ISDN BRI DBM (BKP). |
| | Frame Relay Link | Only frame relay link statistics for the selected interface. |
| | Frame Relay Error | Only frame relay error statistics for the selected interface. |
| | Frame Relay LMI | Only frame relay LMI statistics for the selected interface. |
| | DLCI: *nnnn* | Statistics for the selected DLCI.<br>To select a DLCI:<br>*Main Menu → Status → Performance Statistics → [Network/Port-1/Port-2/BRI-B1] Frame Relay → PVCs → DLCI → nnnn* |
| Port-1 only | Comp, DLCI: *nnnn* | Compression statistics for the selected DLCI. |
| [1] BRI selections only appear when an ISDN BRI DBM is installed and enabled. | | |

When Clear completes, Command Complete appears at the bottom of the screen, unless you are clearing a DLCI's statistics. When statistics for a DLCI are cleared, no message appears.

# Troubleshooting Problem Tables

The FrameSaver access unit is designed to provide you with many years of trouble-free service. If a problem occurs, however, refer to the appropriate table in the following sections for possible solutions.

## Access Unit Problems

| Symptom | Possible Cause | Solutions |
|---|---|---|
| No power, or the LEDs are not lit. | The power cord is not securely plugged into the wall receptacle to rear panel connection. | Check that the power cord is securely attached at both ends. |
| | The wall receptacle has no power. | ■ Check the wall receptacle power by plugging in some equipment that is known to be working.<br>■ Check the circuit breaker.<br>■ Verify that your site is not on an energy management program. |
| Power-Up Self-Test fails. Only Alarm LED is on after power-up. | The access unit has detected an internal hardware failure. | 1. Reset the access unit and try again.<br>2. Return the access unit to the factory (refer to *Warranty, Sales and Service Information* on Page A of this document).<br>3. Contact your service representative. |
| Cannot access the access unit or the user interface. | Login or password is incorrect, COM port is misconfigured, or the access unit is otherwise configured so it prevents access. | ■ Reset the access unit (see *Resetting the Access Unit's COM Port or Factory Defaults* on page 5-15).<br>■ Contact your service representative. |
| Device Fail appears on the System and Test Status screen under Self-Test results. | The access unit detects an internal hardware failure. | Record the 8-digit code from the System and Test Status screen, then contact your service representative. |
| An LED appears dysfunctional. | LED is burnt out. | Run the Lamp Test. If the LED in question does not flash with the other LEDs, then contact your service representative. |

| Symptom | Possible Cause | Solutions |
|---|---|---|
| Not receiving data; access unit appears to be stuck. | ■ DDS line rate/speed has changed.<br>■ Excessive BPVs causing access unit to become stuck in Autobaud mode.<br>■ Excessive Loop Loss causing access unit to become stuck in Autobaud mode. | 1. Verify that your subscriber loop is running at 56 or 64CC kbps.<br>2. If getting Excessive BPVs, verify that you do not have a bad cable. If the cable is good, contact the network provider.<br>3. If getting excessive Loop Loss (dB) indications, install a shorter cable.<br>4. Access the Interface Status screen and select Network.<br>– If the DDS Line Rate (kbps) field shows Autobaud, then the access unit may be stuck in Autobaud mode.<br>– Monitor how long the access unit stays in Autobaud mode. If DDS Line Rate (kbps) does not change to a line rate within a reasonable period of time, then the access unit is stuck in Autobaud mode.<br>– If stuck in Autobaud mode, configure DDS Line Rate (kbps) for 56 or 64 kbps. |
| Not receiving data. | Network cable loose or broken.<br>DDS network is down. | Reconnect or repair the cable.<br>Call the network service provider. |
| Receiving data errors on a multiplexed DLCI, but frame relay is okay. | FR Discovery is being used for automatic DLCI and PVC configuration, and the equipment at the other end is not frame relay RFC 1490-compliant. | Change the DLCI Type for each network DLCI from Multiplexed to Standard, turning off multiplexing. |

## Data Compression Problems

| Symptom | Possible Cause | Solutions |
|---|---|---|
| Compression Connection Failure Alarm or Trap. | The underlying DLCI is not operative. | Refer to *Troubleshooting Problem Tables*, *Frame Relay PVC Problems*, on page 5-22. |
| | The underlying DLCI does not have Compression enabled. | Configure Compression for DLCI. |
| | Compression is not configured at both ends of the PVC. | Set the Compression configuration option to Enable at both ends. |
| | Both access units on the PVC do not have the same compression mode. | Configure both access units so their Compression configuration options are compatible. |
| Low Compression Ratio Alarm, Status, or Trap. | Compression Ratio Alarm Threshold setting is not realistic given the compression capability of the data content. | Increase the Alarm Threshold configuration option setting, then verify that a realistic alarm threshold is chosen. |
| | There is a high percentage of short packets with Short Packet Bypass enabled. | Raise the Alarm Threshold configuration option setting, then disable Short Packet Bypass.<br>**NOTE:** Disabling Short Packet Bypass may decrease performance. |
| Low Throughput for PVC. | Compression Flow Control method is incompatible with the DTE. | Select a flow control method that is compatible with the DTE. Selecting the Clock setting yields the best throughput. |
| | There is insufficient port clock rate. | Increase the communication port's speed using the Port Rate (Kbps) configuration option setting. |
| | There is a high error rate across the PVC. The network is discarding packets due to an excessive burst rate. | Correct the source of the errors, or increase the CIR (bps) setting. Make sure that the Inbound and Outbound CIR Enforcement Modes are compatible with burst rates. |

## Frame Relay PVC Problems

| Symptom | Possible Cause | Solutions |
|---|---|---|
| No receipt or transmission of data. | Cross Connection of the DLCIs are configured incorrectly. | Verify the PVC connections, DLCIs, and CIRs agree with those of the service provider. |
| | DLCI is inactive on the frame relay network. | Verify that DLCI(s) is active on the PVC Connection Status screen. If DLCI(s) is not active, contact the service provider.<br>Verify the LMI Reported DLCI field on the Interface Status screen. |
| | DTE is configured incorrectly. | Check the DTE's configuration. |
| | LMI is not configured properly for the DTE or network. | Configure LMI characteristics to match those of the DTE or network. |
| | LMI is not configured properly for the DTE, network, or BRI channel. | Configure LMI characteristics to match those of the DTE, network, or BRI channel. |
| | LMI link is inactive. | Verify that the LMI link is active on the network; the Network Performance Statistics status messages received will increment. |
| Losing Data. | CIR and Excess Burst Size is incorrectly configured. | Verify the Network and Port CIR and Excess Burst Size agree with those of the service provider. |
| | Frame relay network is experiencing problems. | Run PVC Loopback and Pattern tests to isolate the problem, then contact the service provider. |

### ISDN BRI DBM Problems

Refer to the Last Cause Values in Chapter 5 of the User's Guide, *Maintenance and Troubleshooting*, for more information about ISDN problems. Refer to Chapter 4, *Setting Up*, for more information about configuration.

| Symptom | Possible Cause | Solutions |
|---|---|---|
| Cannot connect to remote unit | Misconfiguration | 1. Check that the call profile is correct on both units.<br>2. Check that the remote unit is configured to answer.<br>3. Check that autobackup is enabled and no time restrictions apply. |
| BRI LMI comes up, but no data is transferred | Misconfiguration | Check that the DLCI numbers are correct and are the same at both ends. |

## Tests Available

The Test menu allows you to run loopbacks and test patterns on the FrameSaver access unit, and to test the front panel LEDs. It is available to users with a security access level of 1 or 2. From the Test menu:

| To access . . . | Select . . . |
|---|---|
| PVC tests for the network interface | Network PVC Tests[1] |
| PVC tests for Port 1 | Port-1 PVC Tests[1] |
| PVC tests for Port 2 | Port-2 PVC Tests[1] |
| PVC tests for B channel | BRI PVC Tests[1] |
| Physical tests for the Network interface | Network Physical Tests |
| Physical tests for Port 1 | Port-1 Physical Tests |
| Physical tests for Port 2 | Port-2 Physical Tests |
| Device Tests for the access unit | Device Tests |
| [1] PVC Tests menu selections are suppressed when there are no PVCs defined for the interface. | |

The following table matrix shows which tests can be run concurrently. It shows physical tests run with other physical tests, physical tests run with logical tests, and logical tests run with other logical tests.

- The CSU and DSU loopbacks and 511 generation/monitor test are supported on the DDS network interface.
- The external DTE loopback and 511 pattern generation/monitor are supported on the DTE ports.

**Test Matrix (1 of 4)**

| **Test Category: *Physical and Physical*** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Test Type:** ***Physical*** | | Local Loopbacks | | | | Pattern Tests | | |
| ***Physical*** | **Test:** | Network CSU Loopback | Network DSU Loopback | Port-1 DTE External Loopback | Port-2 DTE External Loopback | Network Send/ Monitor 511 | Port-1 Send/ Monitor 511 | Port-2 Send/ Monitor 511 |
| Local Loopbacks | CSU Loopback | N | N | Y | Y | N | N | N |
| | DSU Loopback | N | N | Y | Y | N | N | N |
| | Port-1 DTE External Loopback | Y | Y | N | Y | Y | Y | Y |
| | Port-2 DTE External Loopback | Y | Y | Y | N | Y | Y | Y |
| Pattern Tests | Network Send/ Monitor 511 | N | N | Y | Y | Y [1] | Y | Y |
| | Port-1 Send/ Monitor 511 | Y | Y | N | Y | Y | Y [1] | Y |
| | Port-2 Send/ Monitor 511 | Y | Y | Y | N | Y | Y | Y [1] |

[1] As long as one end of the circuit is sending and the other end is monitoring the pattern. You cannot send or monitor two patterns.

Coordinate with your service provider when running physical tests. Most end-to-end physical tests do not work on a frame relay network.

**Test Matrix (2 of 4)**

| **Test Category: *Physical and Logical*** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Test Type:** ***Physical*** | | Local Loopbacks | | | | Pattern Tests | | |
| ***Logical*** | **Test:** | Network CSU Loopback | Network DSU Loopback | Port-1 DTE External Loopback | Port-2 DTE External Loopback | Network Send/ Monitor 511 | Port-1 Send/ Monitor 511 | Port-2 Send/ Monitor 511 |
| PVC Loopbacks | Network DLCI *nnnn* Loopback | N | N | Y | Y | N | Y | Y |
| | Port-1 DLCI *nnnn* Loopback | Y | Y | N | Y | Y | N | Y |
| | Port-2 DLCI *nnnn* Loopback | Y | Y | Y | N | Y | Y | N |
| | BRI DLCI *nnnn* Loopback | Y | Y | Y | Y | Y | Y | Y |
| Pattern Tests | Network DLCI *nnnn* Send Pattern | N | N | Y | Y | N | Y | Y |
| | Network DLCI *nnnn* Monitor Pattern | N | N | Y | Y | N | Y | Y |
| | Port-1 DLCI *nnnn* Send Pattern | Y | Y | N | Y | Y | N | Y |
| | Port-1 DLCI *nnnn* Monitor Pattern | Y | Y | N | Y | Y | N | Y |
| | Port-2 DLCI *nnnn* Send Pattern | Y | Y | Y | N | Y | Y | N |
| | Port-2 DLCI *nnnn* Monitor Pattern | Y | Y | Y | N | Y | Y | N |
| | BRI DLCI *nnnn* Send Pattern | Y | Y | Y | Y | Y | Y | Y |
| | BRI DLCI *nnnn* Monitor Pattern | Y | Y | Y | Y | Y | Y | Y |
| Connectivity | Network DLCI *nnnn* | N | N | Y | Y | N | Y | Y |
| | Port-1 DLCI *nnnn* | Y | Y | N | Y | Y | N | Y |
| | Port-2 DLCI *nnnn* | Y | Y | Y | N | Y | Y | N |
| | BRI DLCI *nnnn* | Y | Y | Y | Y | Y | Y | Y |

**Test Matrix (3 of 4)**

| **Test Category: *Logical and Logical*** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Test Type:** ***Logical*** | | PVC Loopbacks | | | | Connectivity | | | |
| ***Logical*** | **Test:** | Network DLCI *nnnn* Loopback | Port-1 DLCI *nnnn* Loopback | Port-2 DLCI *nnnn* Loopback | BRI DLCI *nnnn* Loopback | Network DLCI *nnnn* | Port-1 DLCI *nnnn* | Port-2 DLCI *nnnn* | BRI DLCI *nnnn* |
| PVC Loopbacks | Network DLCI *nnnn* Loopback | Y [2] | Y | Y | Y | Y [2] | Y | Y | Y |
| | Port-1 DLCI *nnnn* Loopback | Y | Y [2] | Y | Y | Y | Y [2] | Y | Y |
| | Port-2 DLCI *nnnn* Loopback | Y | Y | Y [2] | Y | Y | Y | Y [2] | Y |
| | BRI DLCI *nnnn* Loopback | Y | Y | Y | Y [2] | Y | Y | Y | Y [2] |
| Pattern Tests | Network DLCI *nnnn* Send Pattern | Y [2] | Y | Y | Y | Y [2] | Y | Y | Y |
| | Network DLCI *nnnn* Monitor Pattern | Y [2] | Y | Y | Y | Y [2] | Y | Y | Y |
| | Port-1 DLCI *nnnn* Send Pattern | Y | Y [2] | Y | Y | Y | Y [2] | Y | Y |
| | Port-1 DLCI *nnnn* Monitor Pattern | Y | Y [2] | Y | Y | Y | Y [2] | Y | Y |
| | Port-2 DLCI *nnnn* Send Pattern | Y | Y | Y [2] | Y | Y | Y | Y [2] | Y |
| | Port-2 DLCI *nnnn* Monitor Pattern | Y | Y | Y [2] | Y | Y | Y | Y [2] | Y |
| | BRI DLCI *nnnn* Send Pattern | Y | Y | Y | Y [2] | Y | Y | Y | Y [2] |
| | BRI DLCI *nnnn* Monitor Pattern | Y | Y | Y | Y [2] | Y | Y | Y | Y [2] |
| Connectivity | Network DLCI *nnnn* | Y [2] | Y | Y | Y | Y [2] | Y | Y | Y |
| | Port-1 DLCI *nnnn* | Y | Y [2] | Y | Y | Y | Y [2] | Y | Y |
| | Port-2 DLCI *nnnn* | Y | Y | Y [2] | Y | Y | Y | Y [2] | Y |
| | BRI DLCI *nnnn* | Y | Y | Y | Y [2] | Y | Y | Y | Y [2] |
| [2] Tests can be run together as long as they are run on different DLCIs. | | | | | | | | | |

**Test Matrix (4 of 4)**

| **Test Category: *Logical and Logical*** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Test Type:** ***Logical*** | | Pattern Tests | | | | | | | |
| ***Logical*** | **Test:** | Network DLCI *nnnn* Send Pattern | Network DLCI *nnnn* Monitor Pattern | Port-1 DLCI *nnnn* Send Pattern | Port-1 DLCI *nnnn* Monitor Pattern | Port-2 DLCI *nnnn* Send Pattern | Port-2 DLCI *nnnn* Monitor Pattern | BRI DLCI *nnnn* Send Pattern | BRI DLCI *nnnn* Monitor Pattern |
| PVC Loopbacks | Network DLCI *nnnn* Loopback | Y [2] | Y [2] | Y | Y | Y | Y | Y | Y |
| | Port-1 DLCI *nnnn* Loopback | Y | Y | Y [2] | Y [2] | Y | Y | Y | Y |
| | Port-2 DLCI *nnnn* Loopback | Y | Y | Y | Y | Y [2] | Y [2] | Y | Y |
| | BRI DLCI *nnnn* Loopback | Y | Y | Y | Y | Y | Y | Y [2] | Y [2] |
| Pattern Tests | Network DLCI *nnnn* Send Pattern | Y [2] | Y | Y | Y | Y | Y | Y | Y |
| | Network DLCI *nnnn* Monitor Pattern | Y | Y [2] | Y | Y | Y | Y | Y | Y |
| | Port-1 DLCI *nnnn* Send Pattern | Y | Y | Y [2] | Y | Y | Y | Y | Y |
| | Port-1 DLCI *nnnn* Monitor Pattern | Y | Y | Y | Y [2] | Y | Y | Y | Y |
| | Port-2 DLCI *nnnn* Send Pattern | Y | Y | Y | Y | Y [2] | Y | Y | Y |
| | Port-2 DLCI *nnnn* Monitor Pattern | Y | Y | Y | Y | Y | Y [2] | Y | Y |
| | BRI DLCI *nnnn* Send Pattern | Y | Y | Y | Y | Y | Y | Y [2] | Y |
| | BRI DLCI *nnnn* Monitor Pattern | Y | Y | Y | Y | Y | Y | Y | Y [2] |
| Connectivity | Network DLCI *nnnn* | Y [2] | Y [2] | Y | Y | Y | Y | Y | Y |
| | Port-1 DLCI *nnnn* | Y | Y | Y [2] | Y [2] | Y | Y | Y | Y |
| | Port-2 DLCI *nnnn* | Y | Y | Y | Y | Y [2] | Y [2] | Y | Y |
| | BRI DLCI *nnnn* | Y | Y | Y | Y | Y | Y | Y [2] | Y [2] |
| [2] Tests can be run together as long as they are run on different DLCIs. | | | | | | | | | |

Refer to Chapter 5, *Device Error*, of the *FrameSaver 9620 User's Guide* to interpret test messages.

# PVC Tests

PVC tests can be run on the following interfaces for the requested DLCI:

- Network
- Port (1 and 2)
- BRI-B1

Loopback, and send/monitor pattern tests are available for each interface on the selected DLCI. FrameSaver access units should be at each end of the circuit. If a PVC Loopback is started at one end of the circuit, the other end can send and monitor pattern tests.

**CAUTION:**

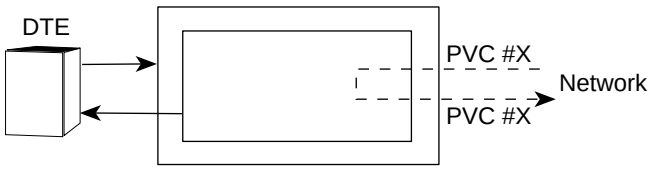
**PVC tests between 9x20/9x21 FrameSaver access units on a multiplexed DLCI are non-disruptive to data, and data can be sent while a test is running. If the device at one end of the circuit is not a 9x20/9x21 unit, these tests are disruptive to data.**

## Network/Port/BRI (Internal) PVC Loopback

The Network/Port/BRI PVC Loopback (Internal) loops frames back to the selected interface on a per-PVC basis. This test logically (not physically) loops back frames from one FrameSaver access unit node through the frame relay PVC to the same access unit node.

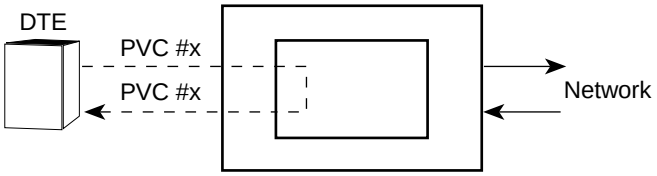
*Main Menu → Test → [Network, Port-1, Port-2, or BRI-B1] PVC Tests → PVC Loopback*

**Network** PVC L**oo**p**b**a**c**k

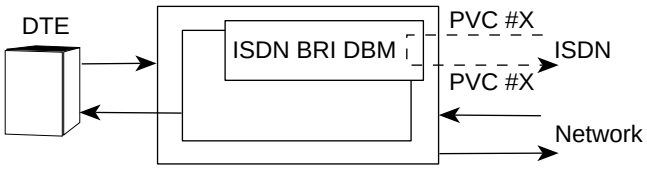



| If the selected DLCI is . . . | Then the PVC Loopback is . . . |
|---|---|
| Standard | Disruptive |
| Proprietary, multiplexed | Nondisruptive |

Port PVC Loopback




BRI PVC Loopback




**NOTE:**

PVC tests cannot be run and will not appear for a Port-1 DLCI that is configured for compression (see the DLCI Compression option in *Configuring DLCI Records for Each Interface* in Chapter 4).

## Send Pattern

This test sends packets filled with a hexadecimal 55 test pattern and sequence number over the selected interface on a per-DLCI basis.

*Main Menu → Test → [Network/Port-1/Port-2/BRI-B1] PVC Tests → Send Pattern*

| If the selected DLCI is . . . | Then the Send Pattern test is . . . |
|---|---|
| Standard | Disruptive |
| Proprietary, multiplexed | Nondisruptive |

### Monitor Pattern

This test monitors packets for the 55 hexadecimal test pattern and checks sequence numbers using a proprietary method. To view the test results, see the PVC Tests [Network, Port-1/Port-2, or BRI-B1] DLCI screen.

*Main Menu → Test → [Network, Port-1, Port-2, or BRI-B1] PVC Tests → Monitor Pattern*

The current number of sequence and data errors are shown under the Result column when the FrameSaver access unit is in sync. An **Out of Sync** message appears when 5 packets out of 25 are missing or out of sequence.

These error counts are updated every second. If the maximum count is reached, **99999+** appears in the fields.

### Connectivity

Connectivity is a proprietary method that determines whether the FrameSaver access unit node at the other end of the frame relay PVC is active. This test stops automatically and can only be executed for circuit multiplexed PVCs.

*Main Menu → Test → [Network, Port-1, Port-2, or BRI-B1] PVC Tests → Connectivity*

Selecting Connectivity sends a packet to the FrameSaver access unit at the other end of the PVC. A response received within 5 seconds indicates that the access unit at the remote end is alive (operational and connected), and the round trip (RT) time is shown in milliseconds (ms), with a resolution of 10 ms. If a response is not received within 5 seconds, **No Response** appears in the Result column.

## Physical Tests

Physical Tests can be commanded from any of the following interfaces:

- Network
- Ports 1 and 2

Physical tests require the participation of your network service provider.

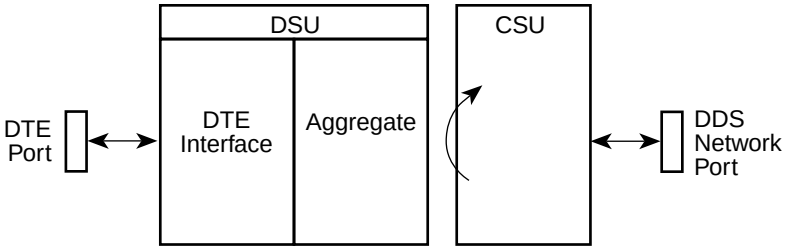
**CAUTION:**

**You should not run these tests with frame relay equipment attached; you must disconnect the frame relay equipment and use external test equipment.**

## CSU (External) Network Loopback

CSU Loopback loops the received signal on the network interface back to the network. This loopback is an external loopback that is located as close as possible to the network interface.

*Main Menu → Test → Network Physical Tests → CSU Loopback*



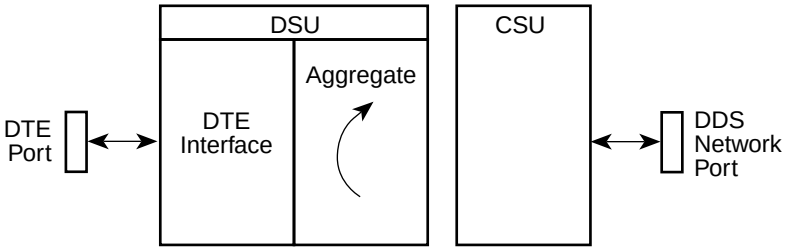

### CAUTION:

**This test may affect the operation of the PVCs assigned to the network interface. In addition, IP data sent over the PVC will be disrupted while this test is active.**

## DSU (Internal) Network Loopback

DSU loopback loops the received signal on the network interface back to the network without affecting operation of other ports. The signal is looped on the DTE side of the FrameSaver access unit. This loopback is an internal loopback that is located as close as possible to the customer interface serving the DTE.

*Main Menu → Test → Network Physical Tests → DSU Loopback*



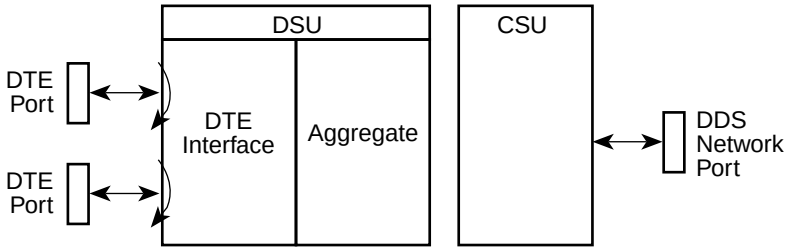

### CAUTION:

**This test may affect the operation of the PVCs assigned to the network interface. In addition, IP data sent over the PVC will be disrupted while this test is active.**

## DTE External Port Loopback

DTE External Loopback loops the user data port back to the DTE interface on a per-port basis without affecting operation of the remaining ports. This loopback is located as close as possible to the customer interface. Use this loopback for isolating problems on the DTE port interface. An attached device or test equipment must generate data to be looped back.

*Main Menu → Test → [Port-1 or Port-2] Physical Tests → DTE External Loopback*




FrameSaver Access Unit

497-14931-01

**CAUTION:**

**This test may affect the operation of the PVCs assigned to this port. In addition, IP data sent over the PVC will be disrupted while this test is active.**

## Send 511

This test sends the 511 test pattern over the selected interface. The 511 test pattern is a pseudo-random bit sequence (PRBS) that is 511 bits long (on the data ports only). This is a PRBS $2^9$ –1 test.

*Main Menu → Test → [Network, Port-1, or Port-2] Physical Tests → Send 511*

When sending or monitoring a 511 test pattern using an external loopback connector on the network or DTE port, you must follow the sequence below for these tests to run correctly.

### ▶ Procedure

To send a 511 test pattern using an external loopback connector:

1. Remove the network cable so that a No Signal (NS) condition occurs.
2. Start the Send Pattern test.
3. Place the loopback cable on the network or DTE port interface.
4. Start the Monitor 511 test.

### Monitor 511

For Monitor 511, a 511 test pattern being sent over the network or DTE port interface can be monitored. To view the test results, see the Network or Port-*n* Physical Tests screen.

*Main Menu → Test → [Network, Port-1, or Port-2] Physical Tests → Monitor 511*

The current number of bit errors is shown under the Result column when the FrameSaver access unit is in sync. An Out of Sync message appears when the test pattern generator and receiver have not yet synchronized.

This error count is updated every second. If the maximum count is reached, 99999+ is shown in the field.

**NOTE:**

The 511 monitor expects external equipment to provide the clock for the 511 pattern for timing the incoming pattern on interchange circuit DA (ITU 113) – Transmit Signal Element Timing (XTXC), with the DTE as the source.

## Device Tests

The FrameSaver access unit supports a Lamp Test at the device-level:

- **Lamp Test** – Use this non-disruptive test to determine whether all LEDs are lighting and functioning properly. All LEDs flash or blink on and off at the same time every 1/2 second during execution of the test. When you stop the test, the LEDs are restored to their normal condition. If the Test Timeout configuration option is enabled and a Test Duration is set, the Lamp Test stops when the test duration expires.

See *Setting General Options* in Chapter 4 to configure the unit to automatically end the test.

# Test Timeout

A Test Timeout feature is available to automatically terminate a test (as opposed to manually terminating a test) after it has been running a specified period of time.

It is recommended that this feature be used when the FrameSaver access unit is remotely managed through an inband data stream (PVC). If a test is accidently commanded to execute on the interface providing management access, control is regained when the specified time period expires, automatically terminating the test.

To use this feature, enable the Test Timeout configuration option, and set a duration for the test to run in the Test Duration (min) configuration option (see *Setting General Options* in Chapter 4).

**NOTE:**

These configuration options do not pertain to tests commanded by the:

— Network, such as the network-initiated CSU and DSU Loopbacks.

— DTE, such as the DTE-initiated External Loopback.

## Latching Loopback

A latching loopback is a network-initiated DSU Loopback. Once a DSU Loopback is started, the FrameSaver access unit remains in loopback until it receives the loopback-release sequence from the network.

The latching loopback code is a control sequence (as opposed to a bipolar violation sequence); therefore, user data may cause the FrameSaver access unit to activate the loopback.

Disable the DSU Latching Loopback configuration option to stop the latching loopback when the network did not command the test.

*Main Menu → Configuration → Network → Physical*

# Starting and Stopping a Test

Use this procedure to start, monitor, or abort specific tests. To abort all active tests on all interfaces, see *Aborting All Tests* on page 5-36.

| When the status of a test is . . . | The only command available is . . . |
|---|---|
| Inactive | Start |
| Active | Stop |

Start or stop an individual test using the same procedure.

## ▶ Procedure

To start or stop a test:

1. Follow this menu sequence:

   *Main Menu* → *Test*

2. Select a group of tests for an interface (Network, Port-1, or Port-2 PVC or Physical Tests) and press Return. The selected test screen appears, with the cursor positioned in the Command column of the first line (available test).

3. Select a group of tests for an interface (Network, Port-1, Port-2, or BRI-B1 PVC Test or Network, Port-1, or Port-2 Physical Tests) and press Return. The selected test screen appears, with the cursor positioned in the Command column of the first line (available test).

   Start or Stop appears in the Command column, and Active or Inactive appears in the Status column, based upon that interface's current test status.

   *Example:*
   Selecting Port-1 Physical Tests from the Test menu causes the Port-1 Physical Tests screen to appear. Only the DTE External Loopback can be run from this screen. The cursor is positioned on the Start/Stop field in the Command column.

   **NOTE:**

   The cursor is not positioned in the Command column when Network PVC Tests is selected; it is positioned in the DLCI Number field.

4. Select the test you want to start or stop and press Return. The selected test for the interface changes from Stop to Start, or from Stop to Start, also changing the status of the test.

5. Press Return again to start or stop the test.

### Aborting All Tests

Use the Abort All Tests selection from the Test menu to abort all tests running on all interfaces, with exception to Network- or DTE-initiated loopbacks. To abort individual tests that are active, see *Starting and Stopping a Test* on page 5-35.

#### ▶ Procedure

To abort all tests on all interfaces:

1. Follow this menu sequence:

   *Main Menu* → *Test*

2. Select Abort All Tests and press Return.

   Command Complete appears when all tests on all interfaces have been terminated.

   **NOTE:**

   Abort All Tests does not interrupt Network- or DTE-initiated loopbacks.

## Determining Test Status and Results

Current test status and results are available on the:

- Test screen from where you execute the test
- System and Test Status screen
- NMS
- Test LED

# Downloading Software

The FrameSaver access unit is capable of accepting a software download from a PC through its COM port to support a file transfer or software upgrade. The Download feature is used only by your service representative to update your access unit.

# File Transfer

The FrameSaver access unit supports a standard File Transfer Protocol (FTP) server over Transmission Control Protocol (TCP) to allow you to transfer configuration files *to/from* an access unit node, and transfer program files *to* an access unit node. A complete binary image of the configuration files can be copied to a host to provide a backup. The unit must be configured to support Telnet and FTP Sessions.

Initiate an FTP session to an access unit node in the same way as you would initiate an FTP to any other IP-addressable device.

Be aware of the following rules when doing a file transfer:

- You must have Access Level 1 permission to use the put command.
- You cannot put a file to the factory.cfg file under the system directory.
- You can only put a NAM or DBM program file (nam1_ctl.ocd, nam2_low.ocd, nam3_hi.ocd, or dbmprog.ocd) into an access unit.
- Before putting a download file, you must use the “bin” binary command to place the data connection in Binary mode.
- You cannot upload a NAM or DBM program file from an access unit.

### ▶ Procedure

To initiate an FTP session:

1. Start the FTP client program on your host. For example, on a Unix host, type **ftp**, followed by the IP address of the access unit.
2. If a login and password are required (see *Creating a Login* in Chapter 6, *Security and Logins*), you are prompted to enter them here. The FTP prompt appears.
3. The starting directory is the root directory (/). The following are available in the system memory directory: nam1_ctl.ocd, nam2_low.ocd, nam3_hi.ocd, current.cfg, factory.cfg, cust1.cfg, cust.cfg, and dbmprog.ocd.

   Use the standard FTP commands during the FTP session, as well as the following remote FTP commands.

| Command | Definition |
|---|---|
| cd *directory* | Change the current directory on the access unit to *directory*. |
| dir [*directory*] | Print a a listing of the directory contents in the *directory* directory. If no directory is specified, the current one is used. |
| get *file1* [*file2*] | Copy a file from the remote directory of the access unit node to the local directory on the host (for configuration files only). |
| remotehelp [*command*] | Print the meaning of the command. If no argument is given, a list of all known commands is printed. |
| ls [*directory*] | Print an abbreviated list of the directory contents in the specified directory. If no directory is specified, the current one is used. |
| put *file1* [*file2*] | Copy *file1* from a local directory on the host to *file 2* in the current directory of the access unit. |
| recv *file1* [*file 2*] | Same as a get. |
| send *file1* [*file 2*] | Same as a put. |
| pwd | Print the name of the current directory of the access unit. |
| bin | Places the FTP session in binary-transfer mode. |

# Performing a NAM Upgrade

If you need to upgrade the NAM program code, you must transfer the following files in the order specified by using the **put** command:

1. NAM control file (nam1_ctl.ocd)
2. NAM Program-Low Bank (nam2_low.ocd)
3. NAM Program-Hi Bank (nam3_hi.ocd)

These files must all be the same version (from the same revision level) for a successful download (format: R*xxyyzz[a/b]*.ocd).

**NOTE:**

Upgrades are performed over the COM port only.

### ▶ Procedure

To perform a download:

1. Initiate an FTP session to the device that you are upgrading.
2. Type **bin** to enter binary mode.
3. Type **cd system** to change to the system directory.
4. Perform a put of R*xxyyzz*.ctl to the nam1_ctl.ocd file to start the download. If the control file is valid, the message **nam1_ctl.ocd: File Transfer Complete** displays, the write permission will be set on the nam2_low.ocd, the FTP connection will be closed, and the device will reset and enter Minimum mode (OK LED will be flashing).
5. Re-establish an FTP session to the device.
6. Type **bin** to enter binary mode.
7. Type **cd system** to change to the system directory.
8. Perform a put of R*xxyyzza*.ocd to the nam2_low.ocd file to start the download. If a valid nam2_low.ocd (that is, it has the same revision level as nam1_ctl.ocd) is successfully put and has the proper checksum, then the message **nam2_low.ocd: File Transfer Complete** displays, the file is loaded into system memory, the write permission will be set on the nam3_hi.ocd, the system performs a memory bank switch, the FTP connection will be closed, a reset/reinitialization occurs, and the system will stay in Minimum mode.
9. Re-establish an FTP session to the device.
10. Type **bin** to enter binary mode.

11. Type **cd system** to change to the system directory.
12. Perform a put of R*xxyyzzb*.ocd to the nam3_hi.ocd file to start the download. If a valid nam3_hi.ocd (that is, it has the same revision level as the nam1_ctl.ocd and nam2_low.ocd files) is successfully put and has the proper checksum, then the message **nam3_hi.ocd: File Transfer Complete** displays, the file is loaded into system memory, the write permission will be removed for both the nam2_low.ocd and the nam3_hi.ocd files, the system performs a reset/reinitialization, and the system will be in Normal mode and operating from the new program load. The download has successfully completed.

# Performing a DBM Upgrade

### ▶ Procedure

To perform a DBM upgrade:

1. Initiate an FTP session to the device that you are upgrading.
2. Type **bin** to enter binary mode.
3. Type **cd dbm** to change to the dbm directory.
4. Perform a put of R*xxyyzza*.ocd to the dbmprog.ocd file to start the upgrade.

| If the file is . . . | Then the message . . . |
|---|---|
| Successfully put and has the proper checksum | **dbmprog.ocd: File Transfer Complete** displays. The download has successfully completed. |
| Not successfully put (due to a bad file, an invalid file or the wrong checksum) | **dbmprog.ocd: File Transfer Failed** displays. You must now download another dbmprog.ocd file to the DBM for it to become operational. |

# Security and Logins

# 6

## Introduction

This chapter discusses the various methods of providing access security and tells you how to set each up, followed by instructions for logging in or out once security has been set up. Backup security is also discussed.

## Limiting Access

The FrameSaver access unit provides several methods of security by limiting user access through the following user interfaces:

- Direct Async Terminal Interface
- Telnet
- External Devices
- SNMP

### Limiting Direct Async Terminal Access

The FrameSaver access unit provides the following methods for limiting direct async terminal access on the communication (COM) port:

- Disabling the direct async terminal connection.
- Requiring a user ID or password.
- Assigning an access level to the port.

The Communication Port Options screen provides the configuration options to limit async terminal access on the COM port.

### ▶ Procedure

To limit COM port async terminal access:

1. Follow this menu sequence:

   *Main Menu → Configuration*

2. Select the desired configuration area and press Return.

   *Load Configuration From → [Current Configuration/ Customer Configuration 1/Customer Configuration 2]*

3. Follow this menu sequence, pressing Return after each selection:

   *Configuration Edit/Display → User Interface → Communication Port*

   The Communication Port Options screen appears.

4. Select and set the following configuration options, as appropriate.

| **To . . .** | **Set the configuration option . . .** |
|---|---|
| Disable direct async terminal interface connection | Port Use to Alarms. |
| Require a user ID or password to access the COM port | Login Required to Enable. Note: User ID and password combinations must be defined. Refer to *Creating a Login* on page 6-9. |
| Limit the effective access level to Level 3 or Level 2 [1] | Port Access Level to Level 2 or 3. |
| [1] Make sure you have at least one login with Level 1 security set. | |

   **NOTE:**

   See *Resetting the Access Unit's COM Port or Factory Defaults* in Chapter 5 should you inadvertently be locked out.

5. Press Ctrl-a to switch to the screen function key area.

6. To save changes, select Save and press Return. The Save Configuration To screen appears.

7. Select the configuration area where you want to save the changes to and press Return.

   *Save Configuration To → [Current Configuration/ Customer Configuration 1/Customer Configuration 2]*

   When Save is complete, Command Complete appears at the bottom of the screen.

Refer to Chapter 4, *Setting Up,* for more information about communication port configuration options.

## Limiting Telnet Access

The FrameSaver access unit provides the following methods for limiting access through a Telnet session:

- Disabling Telnet access completely.
- Requiring a user ID or password to login.
- Assigning an access level for the port.

### ▶ Procedure

To limit access through a Telnet Session:

1. Follow this menu sequence:

   *Main Menu → Configuration*

2. Select the desired configuration area and press Return.

   *Load Configuration From → [Current Configuration/ Customer Configuration 1/Customer Configuration 2]*

3. Follow this menu sequence, pressing Return after each selection:

   *Configuration Edit/Display → User Interface → Telnet Session*

   The Telnet Session Options screen appears.

4. Select and set the following configuration options, as appropriate.

| **To . . .** | **Set the configuration option . . .** |
|---|---|
| Disable Telnet | Telnet Session to Disable. |
| Require a user ID or password | Login Required to Enable.<br>**NOTE:** User ID and password combinations must be defined. Refer to *Creating a Login* on page 6-9. |
| Assign an access level for a user ID | Session Access Level to a level 1, 2, or 3. |

5. Press Ctrl-a to switch to the screen function key area.
6. To save changes, select Save and press Return.
7. Select the configuration area where you want to save the changes to and press Return.

   *Save Configuration To → [Current Configuration/ Customer Configuration 1/Customer Configuration 2]*

   When Save is complete, Command Complete appears at the bottom of the screen.

# Backup Security

The FrameSaver access unit equipped with an ISDN BRI DBM uses call screening to avoid accidental or intentional disruption of network traffic. The answering internal ISDN BRI DBM only accepts calls from valid calling identifiers.

Additional security includes:

- **Internal ISDN BRI DBM** – When installed and enabled, the ISDN BRI DBM takes advantage of ISDN services for network backup and Calling Number Identification Service (CNIS) to provide backup security. ISDN assures the integrity of calling party identifiers, and the DBM uses the calling party identifier as the destination DBM or backup partner. No additional security is required.
- **External Backup Device** – Using an external backup device for security, it is expected that the device is frame relay-compliant, and provides security and calling number identification.

# Controlling External COM Port Device Access

The FrameSaver access unit allows you to control whether dial-in access for an external device (modem) is allowed on the communication port. Use the External Device Options screen to set the necessary configuration options to allow dial-in access through the COM port.

### ▶ Procedure

To control dial-in access:

1. Follow this menu sequence:

   *Main Menu → Configuration*

2. Select the desired configuration area and press Return.

   *Load Configuration From → [Current Configuration/ Customer Configuration 1/Customer Configuration 2]*

3. Follow this menu sequence, pressing Return after each selection:

   *Configuration Edit/Display → User Interface → External Device (Com Port)*

   The External Device Options screen appears.

4. Select a setting for the Dial-In Access configuration option.

| To . . . | Set the Dial-In Access configuration option to . . . |
|---|---|
| Enable dial-in access | Enable |
| Disable dial-in access | Disable |

5. Press Ctrl-a to switch to the screen function key area.
6. To save changes, select Save and press Return. The Save Configuration To screen appears.
7. Select the configuration area where you want to save the changes to and press Return.

   *Save Configuration To → [Current Configuration/ Customer Configuration 1/Customer Configuration 2]*

   When Save is complete, Command Complete appears at the bottom of the screen.

Refer to Chapter 4, *Setting Up*, for more information.

# Controlling SNMP Access

The FrameSaver access unit supports SNMP Version 1, which only provides limited security through the use of community names. There are three methods for limiting SNMP access:

- Disabling SNMP access.
- Assigning SNMP community names and access levels.
- Assigning IP addresses of NMSs that can access the access unit.

## Disabling SNMP Access

The General SNMP Options screen provides the configuration option to disable SNMP access to the unit. When this configuration option is disabled, the FrameSaver access unit will not respond to any SNMP messages and will not send SNMP traps.

### ▶ Procedure

To disable SNMP access:

1. Follow this menu sequence:

   *Main Menu → Configuration*

2. Select the desired configuration area and press Return.

   *Load Configuration From → [Current Configuration/ Customer Configuration 1/Customer Configuration 2]*

3. Follow this menu sequence, pressing Return after each selection:

   *Configuration Edit/Display → Management and Communication → General SNMP Management*

   The General SNMP Options screen appears.

4. Set the SNMP Management configuration option to Disable; Disable is the factory default setting.

5. Press Ctrl-a to switch to the screen function key area.
6. Select the configuration area where you want to save the changes to and press Return.

   *Save Configuration To → [Current Configuration/ Customer Configuration 1/Customer Configuration 2]*

   When Save is complete, Command Complete appears at the bottom of the screen.

Refer to Chapter 4, *Setting Up*, for more information about SNMP configuration options.

## Assigning SNMP Community Names and Access Levels

The General SNMP Options screen provides the configuration options that allow the FrameSaver access unit to be managed by an SNMP manager supporting the SNMP protocol. Use this screen to:

- Assign the SNMP community names that are allowed to access the access unit's Management Information Base (MIB).
- Specify the type of access allowed for each SNMP community name.

Whenever an external SNMP manager attempts to access an object in the MIB, the community name must be supplied.

### ▶ Procedure

To assign SNMP community names and access levels:

1. Follow this menu sequence:

   *Main Menu → Configuration*

2. Select the desired configuration area and press Return.

   *Load Configuration From → [Current Configuration/ Customer Configuration 1/Customer Configuration 2]*

3. Follow this menu sequence, pressing Return after each selection:

   *Configuration Edit/Display → Management and Communication → General SNMP Management*

   The General SNMP Management Options screen appears.

4. Select and set the following configuration options, as appropriate.

| To . . . | Set the configuration option . . . |
|---|---|
| Enable SNMP management for the access unit | SNMP Management to Enable. |
| Assign SNMP community names | Community Name 1 and Community Name 2 to a community name text up to 255 characters in length. |
| Assign the type of access allowed for the SNMP community names | Name 1 Access and Name 2 Access to Read or Read/Write. |

5. Press Ctrl-a to switch to the screen function key area.
6. To save changes, select Save and press Return.
7. Select the configuration area where you want to save the changes to and press Return.

   *Save Configuration To →[Current Configuration/ Customer Configuration 1/Customer Configuration 2]*

   When Save is complete, Command Complete appears at the bottom of the screen.

Refer to Chapter 4, *Setting Up*, for more information about SNMP configuration options.

## Limiting SNMP Access Through IP Addresses

The FrameSaver access unit provides an additional level of security by:

- Limiting the IP addresses of the NMSs that can access the FrameSaver access unit.
- Performing validation checks on the IP address of SNMP management systems attempting to access the FrameSaver access unit.
- Specifying the access allowed for the authorized NMS when IP address validation is performed.

The SNMP NMS Security Options screen provides the configuration options that determine whether security checking is performed on the IP address of SNMP management systems attempting to communicate with the unit.

Make sure that the SNMP Management configuration option is set to Enable.

Menu selection sequence:
*Main Menu*→*Configuration*→Desired configuration area→ *Management and Communication*→ *General SNMP Management*→ *General SNMP Options*→*SNMP Management*→*Enable*

### ▶ Procedure

To limit SNMP access through the IP addresses:

1. Follow this menu sequence:

   *Main Menu → Configuration*

2. Select the desired configuration area and press Return.

   *Load Configuration From → [Current Configuration/ Customer Configuration 1/Customer Configuration 2]*

3. Follow this menu sequence, pressing Return after each selection:

   *Configuration Edit/Display → Management and Communication → SNMP NMS Security*

   The SNMP NMS Security Options screen appears.

4. Select and set the following configuration options, as appropriate.

| To . . . | Set the configuration option . . . |
|---|---|
| Enable IP address checking | NMS IP Validation to Enable. |
| Specify the number (between 1 and 10) of SNMP management systems that are authorized to send SNMP messages to the access unit | Number of Managers to the desired number. |
| Specify the IP address(es) that identifies the SNMP manager(s) authorized to send SNMP messages to the access unit | NMS *n* IP Address to the appropriate IP address. |
| Specify the access allowed for an authorized NMS when IP address validates is performed | Access Level to Read or Read/Write. |

5. Press Ctrl-a to switch to the screen function key area.

6. To save changes, select Save and press Return.

7. Select the configuration area where you want to save the changes to and press Return.

   *Save Configuration To → [Current Configuration/ Customer Configuration 1/Customer Configuration 2]*

   When Save is complete, Command Complete appears at the bottom of the screen.

Refer to Chapter 4, *Setting Up*, for more information about SNMP configuration options.

# Creating a Login

A login ID and password is required if security is enabled.* You can define a combination of six login/passwords. Each login must be unique and have a specified access level.

## ▶ Procedure

To create a login ID and password:

1. Follow this menu sequence:

   *Main Menu → Control → Administer Logins*

2. Press Ctrl-a to switch to the screen function key area.
3. Select New and press Return.
4. Enter the login, password, and security level information.

| In the field . . . | Enter the . . . |
|---|---|
| Login ID | ID of 1 to 10 characters. |
| Password | Password from 1 to 10 characters. |
| Re-enter password | Password again to verify that you entered the correct password into the device. |
| Access Level | Access level: 1, 2, or 3. |

5. Press Ctrl-a to switch to the screen function key area.
6. To save login information, select Save and press Return.

   When Save is complete, Command Complete appears in the message area at the bottom of the screen. The cursor is repositioned at the Login ID field, ready for another entry.

Refer to Chapter 4, *Setting Up*, for more information about security and login configuration options.

* Security is enabled by the configuration options Login Required for the Communication Port, and Telnet Login Required or FTP Login Required for a Telnet or FTP Session.

# Deleting a Login

A login record can be deleted.

### ▶ Procedure

To delete a login record:

1. Follow this menu sequence:

   *Main Menu → Control → Administer Logins*

2. Press Ctrl-a to switch to the screen function key area.
3. Select PgUp or PgDn and press Return to page through login pages/records until you find the one to be deleted.
4. Once the correct record is displayed, select DeLete and press Return.
5. To save the deletion, select Save and press Return.

   When the deletion is complete, Command Complete appears in the message area at the bottom of the screen. The number of login pages/records reflects one less record, and the record following the deleted record appears.

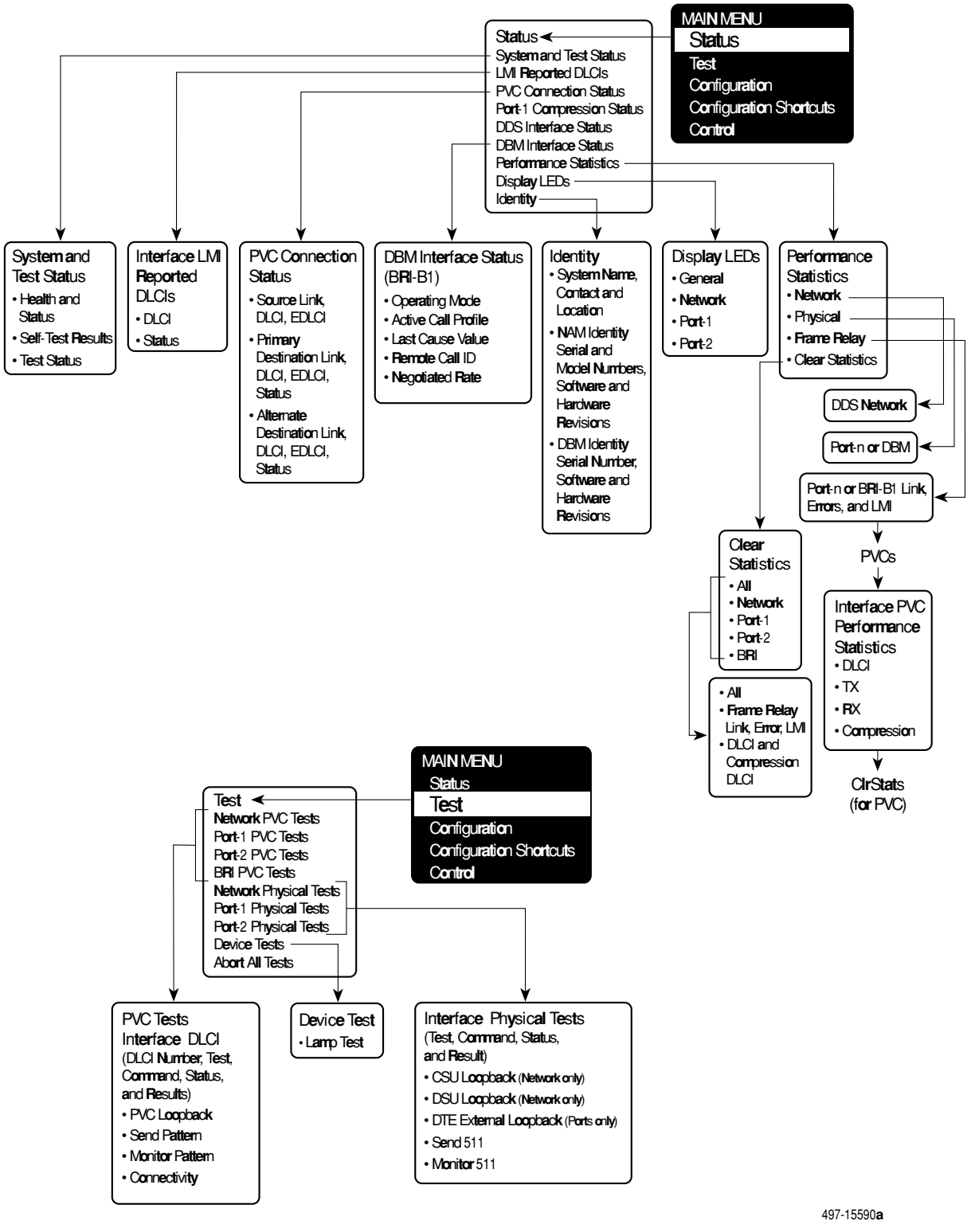
   *Example:*
   Page 2 of 4 is changed to Page 2 of 3.

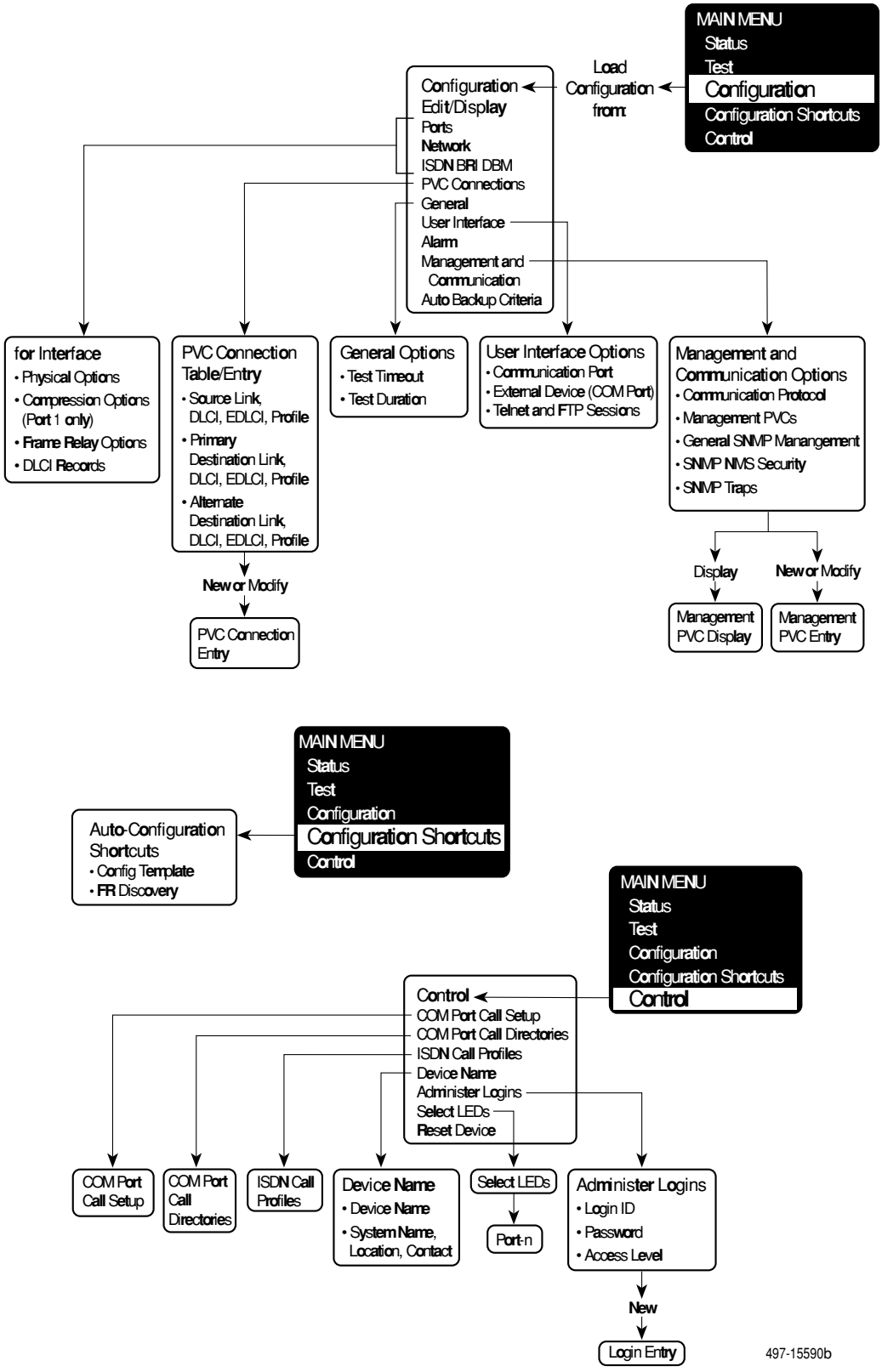
# Menu Hierarchy

# A

## Menus

The following menu structure gives you a graphical representation of how the user interface menus or screens are organized.


MAIN MENU
Status
Test
Configuration
Configuration Shortcuts
Control
Status
System and Test Status
LMI Reported DLCIs
PVC Connection Status
Port-1 Compression Status
DDS Interface Status
DBM Interface Status
Performance Statistics
Display LEDs
Identity
System and Test Status
• Health and Status
• Self-Test Results
• Test Status
Interface LMI Reported DLCIs
• DLCI
• Status
PVC Connection Status
• Source Link, DLCI, EDLCI
• Primary Destination Link, DLCI, EDLCI, Status
• Alternate Destination Link, DLCI, EDLCI, Status
DBM Interface Status (BRI-B1)
• Operating Mode
• Active Call Profile
• Last Cause Value
• Remote Call ID
• Negotiated Rate
Identity
• System Name, Contact and Location
• NAM Identity Serial and Model Numbers, Software and Hardware Revisions
• DBM Identity Serial Number, Software and Hardware Revisions
Display LEDs
• General
• Network
• Port-1
• Port-2
Performance Statistics
• Network
• Physical
• Frame Relay
• Clear Statistics
DDS Network
Port-n or DBM
Port-n or BRI-B1 Link, Errors, and LMI
PVCs
Interface PVC Performance Statistics
• DLCI
• TX
• RX
• Compression
ClrStats (for PVC)
Clear Statistics
• All
• Network
• Port-1
• Port-2
• BRI
• All
• Frame Relay Link, Error, LMI
• DLCI and Compression DLCI
MAIN MENU
Status
Test
Configuration
Configuration Shortcuts
Control
Test
Network PVC Tests
Port-1 PVC Tests
Port-2 PVC Tests
BRI PVC Tests
Network Physical Tests
Port-1 Physical Tests
Port-2 Physical Tests
Device Tests
Abort All Tests
PVC Tests Interface DLCI (DLCI Number, Test, Command, Status, and Results)
• PVC Loopback
• Send Pattern
• Monitor Pattern
• Connectivity
Device Test
• Lamp Test
Interface Physical Tests (Test, Command, Status, and Result)
• CSU Loopback (Network only)
• DSU Loopback (Network only)
• DTE External Loopback (Ports only)
• Send 511
• Monitor 511
497-15590a


MAIN MENU
Status
Test
Configuration
Configuration Shortcuts
Control
Load Configuration from:
Configuration
Edit/Display
Ports
Network
ISDN BRI DBM
PVC Connections
General
User Interface
Alarm
Management and Communication
Auto Backup Criteria
for Interface
• Physical Options
• Compression Options (Port 1 only)
• Frame Relay Options
• DLCI Records
PVC Connection Table/Entry
• Source Link, DLCI, EDLCI, Profile
• Primary Destination Link, DLCI, EDLCI, Profile
• Alternate Destination Link, DLCI, EDLCI, Profile
New or Modify
PVC Connection Entry
General Options
• Test Timeout
• Test Duration
User Interface Options
• Communication Port
• External Device (COM Port)
• Telnet and FTP Sessions
Management and Communication Options
• Communication Protocol
• Management PVCs
• General SNMP Management
• SNMP NMS Security
• SNMP Traps
Display
New or Modify
Management PVC Display
Management PVC Entry
MAIN MENU
Status
Test
Configuration
Configuration Shortcuts
Control
Auto-Configuration Shortcuts
• Config Template
• FR Discovery
MAIN MENU
Status
Test
Configuration
Configuration Shortcuts
Control
Control
COM Port Call Setup
COM Port Call Directories
ISDN Call Profiles
Device Name
Administer Logins
Select LEDs
Reset Device
COM Port Call Setup
COM Port Call Directories
ISDN Call Profiles
Device Name
• Device Name
• System Name, Location, Contact
Select LEDs
Port-n
Administer Logins
• Login ID
• Password
• Access Level
New
Login Entry
497-15590b

# Configuration Worksheets

# B

## Recording Configurations

It is recommended that you keep a record of each FrameSaver access unit's configuration using the configuration worksheets provided in this appendix. Menu-selection sequences are also provided so you can go to the appropriate screens quickly.

### ▶ Procedure

1. Print out or copy the worksheets included in this appendix. Make as many copies of each worksheet as needed.
2. Record the access unit's Device Name on each page.
3. Circle the interface being configured: Port 1, Port 2, Network, or the ISDN BRI DBM, if installed.
4. Write-in or circle the settings for each configuration option.

Do this for each of the alternate configurations stored in Customer Configuration 1 and 2, as well. Store these records for reference, as needed.

Refer to the appropriate configuration sections in Chapter 4, *Setting Up*, for assistance when deciding how to configure the access unit.

### When Using Auto-Configuration Shortcuts

When the Auto-Configuration feature is used, only the local DLCI record and management PVC need to be configured; that is, the PVC connection between the unit and router. By selecting a FR Discovery mode using the Auto-Configuration feature, DLCIs are configured automatically and cross-connected within the unit.

Refer to *Using Configuration Shortcuts* in Chapter 4 for additional information.

# Entering Configurations

Refer to *Configuring the FrameSaver Access Unit* in Chapter 4 when ready to enter your configurations.

# Physical Interface Configuration Worksheets

These worksheets are to record configuration options for the FrameSaver access unit's physical interfaces.

## Network Physical Options Worksheet

Use this worksheet to record the network interface's physical configuration option settings.

*Main Menu* →*Configuration* →*Network* →*Physical*

| **Device Name:** | Refer to Network Physical Configuration Option Table 4-3 |
|---|---|
| **Configuration Option** | **Setting** *Default in [**Bold**]* |
| Operating Mode | [**DDS**], LADS |
| DDS Line Rate (kbps) | 56, 64CC, [**Autobaud**] |
| LADS Timing | Internal, [**Receive**] |
| DSU Latching Loopback | [**Enable**], Disable |
| Cross Pair Detection Alarm | [**Enable**], Disable |
| No Signal Alarm | [**Enable**], Disable |
| Out of Service Alarm | [**Enable**], Disable |
| Out of Frame Alarm | [**Enable**], Disable |
| Excessive BPV Alarm | [**Enable**], Disable |

## Port Physical Options Worksheet

Use this worksheet to record each port's physical configuration option settings.

*Main Menu → Configuration → Ports → [Port-1/Port-2]→ Physical*

| **Device Name:** | Refer to Port Options Table 4-1 |
|---|---|
| **Configuration Option** | **Setting** *Default in [**Bold**]* |
| **Port 1** | |
| Port-1 | [**Enable**], Disable |
| Port Type | EIA-232, [**V.35**] |
| Port Rate (Kbps)<br><br>with V.35 & Compression enabled: | 4.8, 9.6, 14.4, 16.8, 19.2, 24, 28.8, 38.4, 48, [**56**], and 64 kbps<br>plus 128, 192, and 256 kbps |
| Transmit Clock Source | [**Internal**], External |
| Invert Transmit Clock | Enable, [**Disable**] |
| Port (DTE) Initiated Loopbacks | Local, [**Disable**] |
| Control Leads Supported | Force, DTR, RTS, [**Both**] |
| **Port 2** | |
| Port-2 | [**Enable**], Disable |
| Port Type | EIA-232, [**V.35**] |
| Port Rate (Kbps)<br><br>with V.35 & Compression enabled: | 4.8, 9.6, 14.4, 16.8, 19.2, 24, 28.8, 38.4, 48, [**56**], and 64 kbps<br>plus 128, 192, and 256 kbps |
| Transmit Clock Source | [**Internal**], External |
| Invert Transmit Clock | Enable, [**Disable**] |
| Port (DTE) Initiated Loopbacks | Local, [**Disable**] |
| Control Leads Supported | Force, DTR, RTS, [**Both**] |

## Port-1 Compression Options Worksheet

Use this worksheet to record Port-1 compression configuration option settings.

*Main Menu → Configuration → Ports → Port-1→ Compression*

| **Device Name:** | Refer to Port-1 Compression Configuration Option Table 4-2 |
|---|---|
| **Configuration Option** | **Setting** *Default in [**Bold**]* |
| Compression | Enable, [**Disable**] |
| DTE Type[1] | [**Frame Relay**], Bit Synchronous |
| Compression Ratio Alarm[1] | Enable, [**Disable**] |
| Connection Failure Alarm[1] | Enable, [**Disable**] |
| Flow Control[1] | [**Clock**], CTS, None |
| Short Packet Bypass[1] | [**Enable**], Disable |
| Optimize Based On[1] | [**Throughput**], Latency |
| [1] Not shown when Compression is set to Disable. | |

## ISDN BRI DBM Options Worksheet

If an ISDN BRI DBM is installed, use this worksheet to record its physical configuration option settings.

*Main Menu →Configuration →ISDN BRI DBM*

| **Device Name:** | Refer to ISDN BRI DBM Options Table 4-4 |
|---|---|
| **Configuration Option** | **Setting** *Default in [**Bold**]* |
| BRI-B1 | Enable, [**Disable**] |
| Originate or Answer[1] | [**Originate**], Answer |
| Switch Type[1] | **NI-1** (Display only) |
| BRI-B1 Service Profile ID (SPID)[1] | [3 – 20 digits] |
| BRI-B1 Phone Number[1] | [7 digits] |
| BRI-B1 Manual Link Profile[1] | [8 characters] |
| [1] Not shown when the B channel is set to Disable. | |

Use this worksheet to set up ISDN BRI DBM Call Profiles. Up to three call profiles can be set up.

*Main Menu →Control →ISDN Call Profiles*

| **ISDN Call Profile #:** | |
|---|---|
| **Field Name** | **Entry** |
| ISDN Call Profile #: | |
| Status | Enable, [**Disable**] |
| Destination [up to 8 characters] | |
| ***If the ISDN BRI B channel is set to Originate:*** | |
| Called ID *[up to 36 characters]*<br>*This is the phone number to call.* | |
| ***If the ISDN BRI B channel is set to Answer:*** | |
| Calling ID 1 *[up to 36 characters]*<br>*This is the phone number to accept call.* | |
| Calling ID 2 *[up to 36 characters]*<br>*This is the phone number to accept call.* | |

# Frame Relay Options Configuration Worksheet

Use this worksheet to record network, port, and BRI configuration option settings.

*Main Menu → Configuration → Ports → [Port-1/Port-2]→ Frame Relay*

*Main Menu → Configuration → [Network/BRI-B1 Frame Relay] → Frame Relay*

| **Device Name:** | Refer to Frame Relay Options Table 4-5 |
|---|---|
| **Interface:** Port-1, Port-2, Network, or BRI-B1 *(Circle One)* | |
| **Configuration Option** | **Setting** *Default in [**Bold**]* |
| Link Status [1] | [**Enable**], [**Auto**], Disable |
| Inbound CIR Enforcement Mode | [**Forced**], Standard, Discard |
| Outbound CIR Enforcement Mode | [**Forced**], Standard, Buffered |
| LMI Personality [2] | [**User Side**], [**Network Side**], None [5] |
| LMI Protocol [3,4] | Standard, Annex A, [**Annex D**] |
| LMI Error Event (N2) [3] | 1, 2, [**3**], 4, 5, 6, 7, 8, 9, 10 |
| LMI Clearing Event (N3) [3] | 1, 2, 3, [**4**], 5, 6, 7, 8, 9, 10 |
| LMI Status Enquiry (N1) [3,4] | 1, 2, 3, 4, 5, [**6**], . . . 255 |
| LMI Heartbeat (T1) [3,4] | 5, [**10**], 15, 20, 25, 30 |
| LMI Inbound Heartbeat (T2) [3] | 5, 10, [**15**], 20, 25, 30 |
| LMI N4 Measurement Period (T3) [3] | 5, 10, 15, [**20**], 25, 30 |
| LMI Link Status Change Alarm [3] | [**Enable**], Disable |
| DLCI Status Change Alarm [4] | [**Enable**], Disable |

[1] Enable is the default for data ports and network interface; Auto is the default for an ISDN BRI DBM.

[2] User Side is the default for the network interface and answering BRI B channel; Network Side is the default for data ports and originating BRI B channel.

[3] Not shown when the port's LMI Personality is set to None.

[4] Not shown when the network interface's LMI Personality is set to Network Side.

[5] Not shown for the network interface.

# DLCI Records Configuration Worksheet

Recording DLCI records is not necessary when using the configuration shortcuts FR Discovery feature, which automatically configures these records.

*Main Menu → Configuration → Ports → [Port-1/Port-2]→ DLCI Records*

*Main Menu → Configuration → [Network/ISDN BRI DBM] → DLCI Records*

| **Device Name:** | | Refer to DLCI Records Options Table 4-6 |
|---|---|---|
| **Interface /Link** | **Configuration Option** | **Setting** *Default in [**Bold**]* |
| Port-1, Port-2, Network, BRI | DLCI Number | 16 – 1007 |
| | DLCI Status | [**Active**], Inactive |
| | DLCI Type | [**Standard**], Multiplexed |
| | CIR (bps) | 0 – 64,000 [**56000** for BRI] [**64000** for other interfaces] |
| | Excess Burst Size (Bits) | 0 – 999,999 [**0**] |
| | DLCI Priority | Low, [**Medium**], High |
| | DLCI Compression[1] | Enable, [**Disable**] |
| | DLCI Compression Ratio Alarm Threshold[1] | [**1.0:1**], 2.0:1, 3.0:1, 4.0:1 |
| Port-1, Port-2, Network, BRI | DLCI Number | 16 – 1007 |
| | DLCI Status | [**Active**], Inactive |
| | DLCI Type | [**Standard**], Multiplexed |
| | CIR (bps) | 0 – 64,000 [**56000** for BRI] [64**000** for other interfaces] |
| | Excess Burst Size (Bits) | 0 – 999,999 [**0**] |
| | DLCI Priority | Low, [**Medium**], High |
| | DLCI Compression[1] | Enable, [**Disable**] |
| | DLCI Compression Ratio Alarm Threshold[1] | [**1.0:1**], 2.0:1, 3.0:1, 4.0:1 |

[1] Available on Port 1 only.

# PVC Connection Table Configuration Worksheet

Recording PVC connections is not necessary when using the configuration shortcuts FR Discovery feature, which automatically configures these records. Each ID item in the worksheet includes the Source Link, DLCI/EDLCI, and ISDN Call Profile, as well as the Primary and Alternate Destination Link, DLCI/EDLCI, and ISDN Call Profile.

Use this worksheet to record up to 80 PVC connections. Print or photocopy this page as many times as needed.

*Main Menu → Configuration → PVC Connections → New or Modify*

| **Device Name:** | | | | | Refer to PVC Connections Options Table 4-7 |
|---|---|---|---|---|---|
| **Field** | **PVC ID:** | **PVC ID:** | **PVC ID:** | **PVC ID:** | **PVC ID:** |
| Source Link | | | | | |
| Source DLCI | | | | | |
| Source EDLCI | | | | | |
| Primary Destination Link | | | | | |
| Primary Destination DLCI | | | | | |
| Primary Destination EDLCI | | | | | |
| Alternate Destination Link | | | | | |
| Alternate Destination DLCI | | | | | |
| Alternate Destination EDLCI | | | | | |
| Alternate Destination Profile | | | | | |

# General Options Configuration Worksheet

Use this worksheet to record the general configuration options to limit the time that a a test will run.

*Main Menu* → *Configuration* → *General*

| **Device Name:** | Refer to General Configuration Option Table 4-8 |
|---|---|
| **Configuration Option** | **Setting** *Default in [**Bold**]* |
| Test Timeout | [**Enable**], Disable |
| Test Duration (min) | 1 – 120, [**10**] |

# User Interface Options Configuration Worksheets

Record the settings for the User Interface configuration options on the following worksheets:

- Communication Port Configuration Worksheet
- External Device Configuration Worksheet
- Telnet and FTP Session Configuration Worksheet

## Communication Port Options Worksheet

Use this worksheet to record COM port configuration option settings.

*Main Menu* → *Configuration* → *User Interface* → *Communication Port*

| **Device Name:** | Refer to Communication Port Options Table 4-9 |
|---|---|
| **Configuration Option** | **Setting** *Default in [**Bold**]* |
| Port Use | **[Terminal]**, Net Link, Alarm |
| Port Type | **[Asynchronous]**, Synchronous |
| Data Rate (Kbps) | 9.6, 14.4, **[19.2]**, 28.8, 38.4 |
| Clock Source | **[Internal]**, External |
| RIP | **[None]**, Proprietary |
| Character Length | 7, **[8]** |
| Parity | **[None]**, Even, Odd |
| Stop Bits | **[1]**, 1.5, 2 |
| Ignore Control Leads | **[Disable]**, DTR |
| Login Required | Enable, **[Disable]** |
| Port Access Level | **[Level-1]**, Level-2, Level-3 |
| Inactivity Timeout | Enable, **[Disable]** |
| Disconnect Time (Minutes) | 1 – 60, [**5**] |

## External Device Options Worksheet

Use this worksheet to record configuration option settings for an external device that is connected to the access unit's COM port.

*Main Menu* → *Configuration* → *User Interface* → *External Device (COM Port)*

| **Device Name:** | Refer to External Device (COM Port) Options Table 4-10 |
|---|---|
| **Configuration Option** | **Setting** *Default in [**Bold**]* |
| External Device Commands | **[Disable]**, AT, Other |
| Dial-In Access | Enable, **[Disable]** |
| Connect Prefix | |
| Connect Indication String | |
| Escape Sequence | |
| Escape Sequence Delay (Sec) | **[None]**, 0.2, 0.4, 0.6, 0.8, 1.0 |
| Disconnect String | |

## COM Port Call Setup Worksheet

Use this worksheet to set up COM port call directories.

*Main Menu* → *Control* → *COM Port Call Directories*

| **Device Name:** | |
|---|---|
| **Field Name** | **Entry** |
| Directory Number | 1 |
| Directory Phone Number | |
| Directory Number | 2 |
| Directory Phone Number | |
| Directory Number | 3 |
| Directory Phone Number | |
| Directory Number | 4 |
| Directory Phone Number | |
| Directory Number | 5 |
| Directory Phone Number | |
| Directory Number | A [Primary terminal or printer] |
| Directory Phone Number | |

### Telnet and FTP Session Options Worksheet

Use this worksheet to record configuration option settings that set up access via Telnet sessions.

*Main Menu* → *Configuration* → *User Interface* → *Telnet and FTP Sessions*

| **Device Name:** | Refer to Telnet and FTP Session Options Table 4-11 |
|---|---|
| **Configuration Option** | **Setting** *Default in [**Bold**]* |
| Telnet Session | Enable, **[Disable]** |
| Telnet Login Required | Enable, **[Disable]** |
| Session Access Level | **[Level-1]**, Level-2, Level-3 |
| Inactivity Timeout | Enable, **[Disable]** |
| Disconnect Time (Minutes) | 1 – 60, [**5**] |
| FTP Session | Enable, **[Disable]** |
| FTP Login Required | Enable, **[Disable]** |

## Alarm Options Configuration Worksheet

Use this worksheet to record alarm- and trap-generation configuration options.

*Main Menu* → *Configuration* → *Alarm*

| **Device Name:** | Refer to Alarm Options Table 4-12 |
|---|---|
| **Configuration Option** | **Setting** *Default in [**Bold**]* |
| ASCII Alarm Messages | Com Port, **[Disable]** |
| Alarm & Trap Dial-Out | Enable, **[Disable]** |
| Trap Disconnect | **[Enable]**, Disable |
| Call Retry | Enable, **[Disable]** |
| Dial-Out Delay Time (Min) | 1, 2, 3, 4, **[5]**, 6, 7, 8, 9, 10 |
| Alternate Dial-Out Directory | **[None]**, 1, 2, 3, 4, 5 |

# Management and Communication Configuration Worksheets

Record the settings for the Management and Communication configuration options on the following worksheets:

- Communication Protocol Configuration Worksheet
- Management PVCs Configuration Worksheet
- General SNMP Management Configuration Worksheet
- SNMP NMS Security Configuration Worksheet
- SNMP Traps Configuration Worksheet
- Auto Backup Criteria Configuration Worksheet

## Communication Protocol Options Worksheet

Use this worksheet to record configuration options that enable management communication with the node.

*Main Menu* → *Configuration* → *Management and Communication* → *Communication Protocol*

| **Device Name:** | Refer to Communication Protocol Options Table 4-13 |
|---|---|
| **Configuration Option** | **Setting** *Default in [**Bold**]* |
| Node IP Address | |
| Node Subnet Mask | |
| Default Network Destination | [**None**], COM, *PVCname* |
| ***Communication Port**:* | |
| IP Address | |
| Subnet Mask | |
| Link Protocol | [**PPP**], SLIP |
| Alternate IP Address | |
| Alternate Subnet Mask | |

## Management PVCs Options Worksheet

Use this worksheet to record up to 40 management PVCs. Print or photocopy this worksheet as many times as needed.

Each ID/PVC number item in the worksheet includes an area for the PVC option and setting, as well as the Primary and Alternate PVC option and setting.

*Main Menu* → *Configuration* → *Management and Communication* → *Management PVCs* → *New or Modify*

| **Device Name:** | | | | | Refer to Management PVC Options Table 4-14 |
|---|---|---|---|---|---|
| **Field** | **PVC ID:** | **PVC ID:** | **PVC ID:** | **PVC ID:** | **PVC ID:** |
| Name | | | | | |
| *Interface* IP Address (000.000.000.000)[1] | | | | | |
| *Interface* Subnet Mask (000.000.000.000)[1] | | | | | |
| Primary Link | Network, Port-1, Port-2, BRI-B1, Clear | Network, Port-1, Port-2, BRI-B1, Clear | Network, Port-1, Port-2, BRI-B1, Clear | Network, Port-1, Port-2, BRI-B1, Clear | Network, Port-1, Port-2, BRI-B1, Clear |
| Primary DLCI | | | | | |
| Primary EDLCI | | | | | |
| Alternate Link | | | | | |
| Alternate DLCI | | | | | |
| Alternate EDLCI | | | | | |
| Alternate Profile [2] | | | | | |
| Set DE | Enable, [**Disable**] | | | | |
| RIP [3] | [**None**], [**Prop**] | [**None**], [**Prop**] | [**None**], [**Prop**] | [**None**], [**Prop**] | [**None**], [**Prop**] |

[1] The periods between each set of three digits are considered part of the address field but are not entered.

[2] See the ISDN Call Profile on the Control menu.

[3] None is the default for Ports 1 and 2; Proprietary is the default for network interface.

## General SNMP Management Options Worksheet

Use this worksheet to record the necessary information needed to allow the access unit to be managed as an SNMP agent by an NMS supporting the SNMP protocol.

*Main Menu → Configuration → Management and Communication → General SNMP Management*

| **Device Name:** | Refer to General SNMP Management Options Table 4-15 |
|---|---|
| **Configuration Option** | **Setting** *Default in [**Bold**]* |
| SNMP Management | Enable, [**Disable**] |
| Community Name 1 | [**Public**] |
| Name 1 Access | [**Read**], Read/Write |
| Community Name 2 | |
| Name 2 Access | [**Read**], Read/Write |

## SNMP NMS Security Options Worksheet

Up to 10 SNMP managers can be configured/authorized to send SNMP messages to the access unit or node. Use this worksheet to record SNMP security information for each SNMP Manager.

*Main Menu → Configuration → Management and Communication → SNMP NMS Security*

| **Device Name:** | | | Refer to SNMP NMS Security Options Table 4-16 |
|---|---|---|---|
| **NMS IP Validation** | **SNMP Manager #** | **IP Address** 001.000.000.000[1] | **Access Type** *Default in [**Bold**]* |
| Enable, [**Disable**] | 1 | | [**Read**], Read/Write |
| | 2 | | [**Read**], Read/Write |
| | 3 | | [**Read**], Read/Write |
| | 4 | | [**Read**], Read/Write |
| | 5 | | [**Read**], Read/Write |
| | 6 | | [**Read**], Read/Write |
| | 7 | | [**Read**], Read/Write |
| | 8 | | [**Read**], Read/Write |
| | 9 | | [**Read**], Read/Write |
| | 10 | | [**Read**], Read/Write |

[1] The periods between each set of three digits are considered part of the address field but are not entered.

## SNMP Traps Options Worksheet

Up to 6 SNMP managers can be configured/authorized to receive SNMP traps from the access unit or node. Use this worksheet to record SNMP Trap information for each SNMP Manager.

*Main Menu → Configuration → Management and Communication → SNMP Traps*

| **Device Name:** | | | Refer to SNMP Trap Options Table 4-17 |
|---|---|---|---|
| **SNMP Traps** | **SNMP Trap Manager #** | **IP Address** 001.000.000.000[1] | **Destination** *Default in [**Bold**]* |
| Enable, [**Disable**] | 1 | | [**Default**], COM, *PVCname:* |
| | 2 | | [**Default**], COM, *PVCname:* |
| | 3 | | [**Default**], COM, *PVCname:* |
| | 4 | | [**Default**], COM, *PVCname:* |
| | 5 | | [**Default**], COM, *PVCname:* |
| | 6 | | [**Default**], COM, *PVCname:* |
| **General Traps:** Disable, Warm, AuthFail, [**Both**] | | | |
| **Enterprise Specific Traps:** Enable, [**Disable**] | | | |
| **Link Traps:** Disable, Up, Down, [**Both**] | | | |
| **Link Traps Interfaces:** Network, Ports, [**All**] | | | |
| **DLCI Traps on Interfaces:** Network, Ports, [**All**] | | | |
| [1] The periods between each set of three digits are considered part of the address field but are not entered. | | | |

# Auto Backup Criteria Configuration Worksheet

Indicate on this worksheet whether the ISDN BRI DBM is configured for automatic backup and restoral.

*Main Menu* → *Configuration* → *Auto Backup Criteria*

| **Device Name:** | Refer to Auto Backup Criteria Options Table 4-18 |
|---|---|
| **Configuration Option** | **Setting** *Default in [**Bold**]* |
| Auto Backup | Enable, [**Disable**] |

# MIB Descriptions

# C

The MIB (Management Information Base) descriptions listed here provide clarification for the MIB objects when it is not clear how the object definition in the applicable RFC is related to the FrameSaver access unit. Otherwise, the MIB object is supported as documented in the RFC.

This chapter is organized according to the MIBs supported by the FrameSaver access unit:

- MIB II – RFC 1213 and RFC 1573
- Frame Relay DTEs MIB – RFC 1315
- Frame Relay Service MIB – RFC 1604
- RS-232-Like MIB – RFC 1659
- Enterprise MIB

## MIB II Descriptions, RFC 1213 and RFC 1573

The FrameSaver access unit supports the following MIB II object groups as defined in RFC 1213 and RFC 1573:

- System group
- Interfaces group – Supported for the network DDS interface, synchronous data ports, and the COM port. The Evolution of the Interfaces Group (RFC 1573) is also supported by the access unit. Interface statistics only apply to the COM port.
- IP (Internet Protocol) group
- ICMP (Internet Control Management Protocol) group
- TCP (Transmission Control Protocol) group
- UDP (User Datagram Protocol) group

- Transmission group – Supported on the DDS interfaces using the DDS Enterprise MIB. Supported on the frame relay logical link interfaces (Network, Port-1, Port-2, BRI-B1) using the Frame Relay Services or Frame Relay DTE MIBs. Supported on the synchronous data ports using the RS-232-like MIB. Supported on the COM port using the RS-232-like MIB.
- SNMP (Simple Network Management Protocol) group

## System Group

System Group objects are fully supported by the FrameSaver access unit. The following sections clarify the information accessed when these objects are used. This object is set to display the following string:

*[Company enterprise's name] DDS FRAMESAVER; Model: xxxx; S/W Release: yy.yy.yy; H/W CCA number: zzzz-zzz; Serial number: sssssss*

| Object | What It Does | Setting/Contents |
|---|---|---|
| sysDescr *(system 1)* | Provides a full description of the access unit – its Identity. | [*Company enterprise's name*] DDS FRAMESAVER*;* Model: *xxxx;* S/W Release: *yy.yy.yy;* H/W CCA Number: *zzzz-zzz;* Serial Number: *sssssss* |
| sysObjectID *(system 2)* | Identifies the network management subsystem, based upon access unit's housing. | Object identifier:<br>■ 9620 1-Slot – 1.3.6.1.4.1.[*company enterprise's ID*].1.14.2.4.1.1<br>*Example:* 1.3.6.1.4.1.1795.1.14.2.4.1.1 |
| sysServices *(system 7)* | Indicates the set of services supported. | Functionality supported:<br>■ **physical (1)** – Layer 1 for all interfaces<br>■ **datalink/subnetwork (2)** – Layer 2 (frame relay) for synchronous data ports and the COM port (SLIP/PPP)<br>■ **internet (4)** – Layer 3 (IP) for all management links<br>■ **end-to-end (8)** – Layer 4 (TCP/UDP) for all management links<br>Object will be set to 15 (1+2+4+8). |

## Interfaces Group

The Interfaces Group as defined in RFC 1573 consists of an object indicating the number of interfaces supported by the FrameSaver access unit and an interface table containing an entry for each interface. Since RFC 1573 is an SNMPv2 MIB, it is converted to SNMPv1 for support by the FrameSaver access unit.

The following table provides clarification for objects contained in the Interfaces group when it is not clear how the object definition in RFC 1573 is supported by the FrameSaver access unit.

| Object | Description | Setting/Contents |
|---|---|---|
| ifNumber<br>*(interfaces 1)* | Specifies the number of rows/interfaces for this access unit in the ifTable. | Interfaces included: DDS network, frame relay links, synchronous data ports, BRI bearer channel, and COM port. |
| ifIndex<br>*(ifEntry 1)* | Provides the index to the interface table (ifTable) and to other tables as well.<br>When an unsupported index is entered (e.g., 2), noSuchName is returned. | Indexes and values:<br>■ 1 – COM port<br>■ 2 – ISDN BRI DBM (B Channel 1)<br>■ 3 – Reserved<br>■ 4 – DDS network interface<br>■ 5 – Reserved<br>■ 6 – Data Port 1<br>■ 7 – Data Port 2<br>■ 8 – Frame relay logical link sublayer (network interface)<br>■ 9 – Frame relay logical link sublayer (Port 1 interface)<br>■ 10 – Frame relay logical link sublayer (Port 2 interface).<br>■ 11 – Frame relay logical link sublayer (ISDN BRI DBM B Channel 1) |

| Object | Description | Setting/Contents |
|---|---|---|
| ifDescr<br>*(ifEntry 2)* | Supplies text about the interface. | Text Strings |
| | Interfaces: | Interfaces: |
| | ■ DDS network | ■ Network DDS; DDS FR DSU; Hardware Version: [*CCA number*] |
| | ■ COM port | ■ COM Port; DDS FR DSU; Hardware Version: [*CCA number*] |
| | ■ Data ports (Port 1 and 2) | ■ Synchronous Data Port, Slot: 1, Port *n*; DDS FR NAM; Hardware Version: [*CCA number*] |
| | ■ ISDN BRI DBM (B channel) | ■ ISDN BRI DBM B-Channel: 1; ISDN BRI DBM; Hardware Version: [*CCA number*] |
| | Frame relay logical link sublayers: | Frame relay logical link sublayers: |
| | ■ DTE side | ■ Network DDS of FR DTE; DDS FR DSU; Hardware Version: [*CCA number*] |
| | | ■ Data Port *n* of FR DTE; Slot: 1; Port *n*; DDS FR DSU; Hardware Version: [*CCA number*] |
| | | ■ ISDN BRI B-Channel: 1 of FR DTE; DDS FR DSU; Hardware Version: [*CCA number*] |
| | ■ Service side | ■ Network DDS of FR SERVICE; DDS FR DSU; Hardware Version: [*CCA number*] |
| | | ■ Data Port *n* of FR SERVICE; Slot: 1; Port *n*; DDS FR DSU; Hardware Version: [*CCA number*] |
| | | ■ ISDN BRI B-Channel: 1 of FR SERVICE; ISDN BRI DBM; Hardware Version: [*CCA number*] |

| Object | Description | Setting/Contents |
|---|---|---|
| ifType<br>*(ifEntry 3)* | Identifies the interface type based on the physical/link protocol(s), right below the network layer. | Supported values: |
| | ■ Used for DDS network. | ■ other (1) |
| | ■ Used for BRI channels. | ■ basicISDN(20) |
| | ■ Used for COM port when port configured for PPP. | ■ ppp(23) |
| | ■ Used for COM port when port configured for SLIP. | ■ slip(28) |
| | ■ Used for frame relay sublayers of the DDS network interface, synchronous data ports, and B channel 1 when configured for the DTE side of the frame relay UNI, or when no LMI is configured. | ■ frameRelay(32) |
| | ■ Used for the COM port when the port is not configured as a network communication link, and synchronous data ports when configured as EIA232. | ■ rs232(33) |
| | ■ Used for frame relay sublayers of the DDS network interface, synchronous data ports, and B channel 1 when configured for the Service side of the frame relay UNI, or when no LMI is configured. | ■ frameRelayService(44) |
| | ■ Used for Ports 1 and 2 configured for connection to a V.35 DTE cable. | ■ v35(45) |
| ifMtu<br>*(ifEntry 4)* | Identifies the largest datagram that can be sent or received on an interface. | Interfaces:<br>■ DDS network: 2048<br>■ Ports 1 and 2: 2048<br>■ COM port: 1500<br>■ Frame Relay Sublayers: 2048<br>■ ISDN BRI B channels: 2048<br>■ All other interfaces: 0 |

| Object | Description | Setting/Contents |
|---|---|---|
| ifSpeed<br>*(ifEntry 5)* | Provides the current bandwidth for the interface in bits per second. | Interfaces:<br>■ DDS network – Line rate of 56,000 or 64,000 bps, reflecting the line rate detected by the access unit.<br>■ COM port – Configured data rate for the port.<br>■ Data ports – Configured data rate for the port.<br>■ BRI B channels – Currently negotiated data rate for the B channel if a call has been established, 0 if one has not.<br>■ Service side of UNI – Peak data rate available based on physical sublayer (network, data port, or B channel).<br>■ DTE side of UNI – Peak data rate available based on physical sublayer (network, data port, or B channel). |
| ifAdminStatus<br>*(ifEntry 7)* | Only for data ports and frame relay logical-link sublayers. It is read-only for the COM port and network interface.<br>Enables or disables the interface. | ■ **up(1)** – Enables the interface.<br>■ **down(2)** – Disables the interface. |

| Object | Description | Setting/Contents |
|---|---|---|
| ifOperStatus<br>*(ifEntry 8)* | Specifies the current operational state of the interface. | State of Interface: |
| | ■ DDS network interface | **up(1)** – No alarms<br>**down(2)** – Alarm is active.<br>**testing(3)** – Test is active. |
| | ■ COM port<br>When configured as a communication link, up or down is based on state of link-layer protocol and control leads. | **up(1)** – Always up, unless configured as a network communication link.<br>**down(2)** – No alarms in link-layer protocol.<br>**testing(3)** – Never in a test state. |
| | ■ Data ports | **up(1)** – If the DTE supports DTR, DTR is on for the port. If the DTE does not support DTR, the port is never down.<br>**down(2)** – If the DTE supports DTR, DTR is off.<br>**testing(3**) – Test is active. |
| | ■ BRI Channels (DBM) | **up(1)** – Call is active.<br>**down(2)** – Port is disabled or no call is active.<br>**testing(3)** – Test is active on the interface. |
| | ■ Frame relay DTE side | **up(1)** – LMI is up and frame relay link is enabled.<br>**down(2)** – LMI is down and frame relay link is disabled.<br>**testing(3)** – Test is active for any DLCI on the link. |
| | ■ Frame relay service side | **up(1)** – LMI is up and frame relay link is enabled.<br>**down(2)** – LMI is down and frame relay link is disabled.<br>**testing(3)** – Test is active for any DLCI on the link. |

| Object | Description | Setting/Contents |
|---|---|---|
| ifLastChange *(ifEntry 9)* | Indicates the amount of time the interface has been up and running since it entered its current operational state. | Contains the value of sysUpTime object. |
| Input Counters *(ifEntry 10 to 15)* | Collects input statistics on data received by the interface.[1] | ■ ifInOctets (ifEntry 10 object)<br>■ ifInUcastPkts (ifEntry 11 object)<br>■ ifInNUcastPkts (ifEntry 12 object)<br>■ ifInDiscards (ifEntry 13 object)<br>■ ifInErrors (ifEntry 14 object)<br>■ ifInUnknownProtos (ifEntry 15 object) |
| Output Counters *(ifEntry 16 to 21)* | Collects output statistics on data sent by the interface.[1] | ■ ifOutOctets (ifEntry 16 object)<br>■ ifOutUcastPkts (ifEntry 17 object)<br>■ ifOutNUcastPkts (ifEntry 18 object)<br>■ ifOutDiscards (ifEntry 19 object)<br>■ ifOutErrors (ifEntry 20 object)<br>■ ifOutQLenCirEntry (ifEntry 21 object) |
| ifSpecific *(ifEntry 22)* | Identifies each index in ifIndex. | ■ DDS network – [*Company enterprise's name*].2.24.2.6.2<br>■ COM port – .ios.org.dod.internet.mgmt.mib-2.transmission.rs232<br>■ Data ports – .ios.org.dod.internet.mgmt.mib-2.transmission.rs232<br>■ BRI B1 channels – 0.0<br>■ DTE side of frame relay – .ios.org.dod.internet.mgmt.mib-2.transmission.frame-relay<br>■ Service side of frame relay – .ios.org.dod.internet.mgmt.mib-2.transmission.frnetservMIB |

[1] Applies to the frame relay logical link sublayer on the network and data port interfaces. Also applies to the COM port interface if it is configured as a network communications link.

When COM port is not configured as a network communications link, these statistics will not be collected, and an error status will be sent if access is attempted.

## Extension to Interface Table (ifXTable)

This extension contains additional objects for the interface table. Supports only the following objects:

| Object | Description | Setting/Contents |
|---|---|---|
| ifName<br>*(ifXEntry 1)* | Provides name of the interface. | Interface test strings:<br>■ Network DDS<br>■ COM – COM port<br>■ S01P*n* – Slot 01 Port 1 or 2<br>■ BRI-B1 (BRI B channel 1)<br>■ FR UNI (Frame Relay logical link sublayers) |
| ifLinkUpDown-Trap Enable<br>*(ifXEntry 14)* | Indicates whether linkUp/linkDown or enterprise-specific traps should be generated. | COM port not supported.<br>**NOTE:** SNMP Traps must be enabled for the access unit (see SNMP Trap Options screen – *Main/Configuration/Management and Communication/SNMP Traps*). |
| ifHighSpeed<br>*(ifXEntry 15)* | Automatically inserts the ifSpeed setting for the interface (read-only):<br>■ 0 – 499,999 bps: ifHighSpeed = 0 | All interfaces supported. |
| ifConnector-Present<br>*(ifXEntry 17)* | Indicates whether there is a physical connector for the interface. | ■ **true(1)** – Always have this value for the DDS network, data ports, and COM port interfaces.<br>■ **false(2)** – Always have this value for the BRI B channel and frame relay logical link sublayers. |

## Interface Stack Group

The Interface Stack Group is used by the FrameSaver access unit to show the relationship between a logical interface and a physical interface; that is, between the frame relay DTE or service side of the logical link sublayer and the DDS network or data ports.

The following table provides clarification for objects contained in the Interface Stack group when it is not clear how the object definition in RFC 1573 is supported by the access unit.

| Object | Description | Setting/Contents |
|---|---|---|
| ifStackHigher-Layer *(ifStackEntry1)* | Provides the index that corresponds to the higher sublevel specified by ifStackLowerLayer. | ■ For layer corresponding to physical interface (network, data ports, or BRI channels): Set ifStackHigherLayer to the ifIndex of the corresponding frame relay service side logical link sublayer.<br>■ For layer corresponding to logical interface (frame relay DTE or service side of the logical link sublayer): set ifStackHigherLayer to zero; there is no higher interface. |
| ifStackLower-Layer *(ifStackEntry2)* | Provides the index that corresponds to the lower sublevel specified by ifStackHigherLayer. | ■ For layer corresponding to physical interface: Set ifStackLowerLayer to zero; there is no lower interface.<br>■ For layer corresponding to logical interface: Set ifStackLowerLayer to the ifIndex of the corresponding physical interface (network or data port). |
| ifStackStatus *(ifStackEntry3)* | Specifies the stack group's status compared to the interface's ifOperStatus of the Higher Layer object (frame relay DTE or service side logical link sublayer).<br>Supported as a read-only variable. | ■ When ifStackStatus set to **active** – maps to ifOperStatus set to **up(1)** or **testing(3)**.<br>■ When ifStackStatus set to **not in service** – maps to ifOperStatus set to **down(2)**. |

## Interface Test Table

The FrameSaver access unit uses the Interface Test table to provide access to additional tests such as loopbacks and pattern tests, which are not provided for in the Interfaces Group of MIB II.

| Object | Description | Setting/Contents |
|---|---|---|
| ifTestID<br>*(ifTestEntry 1)* | Provides a unique identifier for the current request of the interface's test.<br><br>Ensures that the results of the test are for that request, in case a test is requested by another SNMP Manager before the results of the first test are received. | Set by an SNMP Manager before the test is started. The access unit then increments the previous value. The value is then checked after the test has completed. |
| ifTestStatus<br>*(ifTestEntry 2)* | Indicates the test status of the interface. | ■ Set to **inUse(2)** by an SNMP Manager before a test is started.<br><br>■ Set to **notInUse(1)** by the access unit when the test has completed. Also set to **notInUse(1)** by the access unit if the SNMP Manager fails to set an ifTestType within 5 minutes. |
| ifTestType<br>*(ifTestEntry 3)* | A control variable used to start/stop user-initiated tests on the interface. Provides the following capabilities:<br><br>■ Start/stop data port loopback<br><br>■ Start/stop test pattern on a data port<br><br>■ Start/stop monitor test on a data port | The following objects use identifiers to control tests on the interface:<br><br>■ noTest (*0*) – Stops the test in progress on the interface.<br><br>■ testLoopExternalDTE (*ifTestType 2*) – Starts an External DTE loopback on the interface. Only supported for the data ports.<br><br>■ testMon511 (*ifTestType 4*) – Starts a Monitor 511 test on the interface. Only supported for the data ports.<br><br>■ testSend511 (*ifTestType 6*) – Starts a Send 511 test on the interface. Only supported for the data ports. |

| Object | Description | Setting/Contents |
|---|---|---|
| ifTestCode *(ifTestEntry 5)* | Contains a code which is more specific about the test results. | Supports the following values:<br>■ none *(ifTestCode 1)* – No further information is available. Used for send pattern/code and loopback tests.<br>■ inSyncNoBitErrors (*ifTestCode 2*) – A 511 monitor pattern test has synchronized on the pattern and has not detected any bit errors.<br>■ inSyncWithBitErrors (*ifTestCode 3*) – A 511 monitor pattern test has synchronized on the pattern and has detected bit errors.<br>■ notInSync (*ifTestCode 4*) – A 511 monitor test pattern has not synchronized on the requested pattern. |
| ifTestOwner *(ifTestEntry 6)* | Used by an SNMP Manager to identify the current owner of the test for the interface. | The SNMP Manager sets the object to its IP address when setting ifTestID and ifTestStatus. |

## Generic Receive Address Table

Not supported by the FrameSaver access unit.

## IP Group

The IP Group objects are supported by the access unit for all data paths that are currently configured to carry IP data to/from the access unit, including the PVCs. All of the objects in the IP Group, except for the IP Address Translation table, are fully supported.

The following table provides clarification for objects contained in the IP group when it is not clear how the object definition in MIB II is supported by the access unit. The IP Address Translation table (ipNetToMediaTable) does not apply and will be empty.

| Object | Description | Setting/Contents |
|---|---|---|
| ipForwarding *(ip 1)* | Specifies whether the access unit is acting as an IP gateway for forwarding of datagram received by, but not addressed to, the access unit. | Supports only the following value:<br>■ **forwarding(1)** – The access unit is acting as a gateway. |
| ipAddrTable *(ip 20)* | The address table. | Supported. |

| Object | Description | Setting/Contents |
|---|---|---|
| ipAdEntAddr<br>*(ipAddrEntry 1)* | An IP address supported by the access unit which serves as an index to the address table. | Indexes for tables must be unique, therefore only one ifIndex can be displayed for each IP address supported by the device. If the same IP address is configured for multiple interfaces, or for default IP addresses, the ipAddrTable will not display all of the interfaces that support a particular IP address. |
| ipAdEntIfIndex<br>*(ipAddrEntry 2)* | If this object has a greater value than the ifNumber, then it refers to a proprietary interface not currently implemented by the MIB II Interface Group. | Index value that uniquely identifies the applicable interface; same as ifIndex. |
| ipRouteTable<br>*(ip 21)* | Supported as read/write. However, use caution when adding or modifying routes.<br><br>If it is absolutely necessary to add a route, they should only be added to the connected device (device closest to the destination). Internal routing mechanisms will propagate the route to the other devices.<br><br>Routes over management PVCs do not appear in the ipRoute table. Access these routes via the Enterprise MIB IP Route Table, page C-40. | To delete a route, set object to **invalid**.<br><br>To modify a route, change fields in the desired entry of the routing table (indexed by ipRouteDest).<br><br>To add a route, specify values for a table entry for which the index (ipRouteDest) does not already exist.<br><br>The following objects *must* be specified:<br><br>■ ipRouteDest *(ipRouteEntry 1)* – Serves as an index to the routing table. Only one route per destination can appear in the table.<br><br>To ensure that no duplicate destinations appear in the routing table, the ipRouteDest object will be treated as described in the IP Forwarding Table MIB (RFC 1354).<br><br>■ ipRouteIfIndex – When setting this object via SNMP, the ipRouteIfIndex value of ifindex defined for a particular device type. |

| Object | Description | Setting/Contents |
|---|---|---|
| ipRouteTable *(Cont'd)* | *(Cont'd)* | Objects to be set to the default value if not specified in the set PDU (used to add a route):<br>■ **ipRouteMetric1** – Defaults to **1 hop**.<br>■ **ipRouteMetric2** – Defaults to current slot for carrier devices and to –1 for standalone devices. Do not specify a value.<br>■ **ipRouteType** – Defaults to indirect.<br>■ **ipRouteMask** – Defaults to what is specified in the MIB description.<br><br>Objects not used:<br>■ ipRouteMetric3, ipRoutemetric4, ipRoutemetric5 – Defaults to **1**.<br>■ ipRouteNextHop – Defaults to **0.0.0.0**.<br><br>Read-only objects:<br>■ ipRouteProto *(ipRouteEntry 9)* – Set to **netmgmt(3)** by the software. May have the following values in the access unit:<br>– **other(1)** – Temporary route added by IP.<br>– **local(2)** – Route added or changed due to User configuration.<br>– **netmgmt(3)** – Route added or changed by SNMP set.<br>– **icmp(4)** – Route added or changed by ICMP.<br>– **rip(8)** – Route added or changed by RIP (or similar proprietary protocol).<br>■ ipRouteAge *(ipRouteEntry 10)* – Reflects the value of the time-to-live for the route (in seconds). Defaults to **999**, which represents a route that will be retained permanently.<br>■ ipRouteInfo – Set to object identifier **{0,0}** since it is not used. |

## ICMP Group

The ICMP Group objects are fully supported.

## TCP Group

The TCP Group objects are fully supported, with exception to the tcpConnState object, which is read only since deleteTCB(12) is not supported.

## UDP Group

The UDP Group objects are fully supported.

## Transmission Group

Objects in the Transmission Group are supported on the DDS network interface, the synchronous data ports, and the COM port. These objects are not defined within MIB II, but rather through other Internet-standard MIB definitions. The following table provides clarification for objects contained in the Transmission group when it is not clear how the object definition is supported by the access unit.

| Object | Description |
|---|---|
| rs232<br>*(transmission 33)* | Supported on the synchronous data ports and on the COM port. Defined by the RS-232-like MIB. |
| frame-relay<br>*(transmission 32)* | Supported on DTE side frame relay interfaces. Defined by the Frame Relay DTEs MIB. |
| frameRelayService<br>*(transmission 44)* | Supported on the Service side frame relay interfaces. Defined by the Frame Relay Service MIB. |

### SNMP Group

The SNMP Group objects that apply to a management agent are fully supported. The following objects apply only to an NMS and return a zero value if accessed.

- snmpInTooBig (snmp 8)
- snmpInNoSuchNames (snmp 9)
- snmpInBadValues (snmp 10)
- snmpInReadOnlys (snmp 11)
- snmpInGenErrs (snmp 12)
- snmpInGetResponses (snmp 18)
- snmpInTraps (snmp 19)
- snmpOutGetRequests (snmp 25)
- snmpOutGetNexts (snmp 26)
- snmpOutSetRequests (snmp 27)

## Frame Relay DTEs MIB Descriptions, RFC 1315

The frame relay object defined by RFC 1315 is supported for both the Network and synchronous data ports when the interface is configured to support the DTE side of the frame relay UNI. An interface is considered to support the DTE side when the LMI Personality is configured for DTE side or None.

The Frame Relay DTEs MIB is composed of the following groups and a global object:

- Data Link Connection Management Interface (DLCMI) group
- Circuit Group
- Error Group

## DLCMI Group

The DLCMI group consists of the Data Link Connection Management Interface table. Clarification for objects contained in this table is provided below.

| Object | Description | Setting/Contents |
|---|---|---|
| frDlcmiState *(frDlcmiEntry 2)* | Corresponds to the LMI Protocol configuration option. The DCLI used to support the LMI is determined indirectly, based on the protocol supported. | Supports the following values:<br>■ **noLmiConfigured (1)** – An LMI is not supported on this interface.<br>■ **LMIRev1 (2)** – The standard LMI is supported on this interface.<br>■ **ansiT1-617-D (3)** – The LMI supported on this interface complies with ANSI T1.617, Annex D.<br>■ **ccitt-Q933-A (4)** – The LMI on this interface complies with CCITT Q.933, Annex A. This value is not supported by the standard MIB. The value for ANSI T1.617, Annex B (4) has been redefined to support CCITT Q.933. |
| frDlcmiAddress *(frDlcmiEntry 3)* | Describes the address format used on the frame relay interface. | Supports only the following value:<br>■ **q922(4)** – Indicates the address format specified by the final Q.922 standard. |
| frDlcmiAddressLen *(frDlcmiEntry 4)* | Describes the address length used on the frame relay interface. | Supports only the following value:<br>■ **two-octets(2)** – Indicates the address length is two octets as specified by the final Q.922 standard. |
| LMI Parameters *(frDlcmiEntry 5 to frDlcmiEntry 8)* | Contains the protocol parameters that control the LMI link for the frame relay interface. | If an LMI is configured on the interface, the objects will return the following configured values:<br>■ frDlcmiErrorPollingInterval (*frDlcmiEntry 5*) – LMI Heartbeat (T1) configuration option from 5 to 30, in increments of 5.<br>■ frDlcmiFullEnquiryInterval (*frDlcmiEntry 6*) – LMI Status Enquiry (N1) configuration option.<br>■ frDlcmiErrorThreshold (*frDlcmiEntry 7*) – LMI Error Event (N2) configuration option.<br>■ frDlcmiMonitoredEvents (*frDlcmiEntry 8*) – LMI Clearing Events (N3) configuration option. |

| Object | Description | Setting/Contents |
|---|---|---|
| frDlcmiMax SupportedVCs *(frDlcmiEntry 9)* | Contains the maximum number of virtual circuits allowed for this frame relay interface. The maximum number of virtual circuits for all frame relay interfaces supported by the FrameSaver access unit is 40. This number cannot be changed through this object. | Supported as read-only for all frame relay interfaces. |
| frDlcmiMultiCast *(frDlcmiEntry 10)* | Indicates whether the frame relay interface is using a multicast service. | Supports only the following value:<br>■ **nonBroadcast(1)** – Only point-to-point connections are supported. |

## Circuit Group

The Circuit Group consists of the Circuit Table. This table contains an entry for each virtual circuit (defined by DLCI number) supported on a specific frame relay interface (identified by ifEntry). This table contains any entry for a specific DLCI only when a DLCI record has been created for it. The creation and deletion of DLCIs through the Circuit Table is not currently supported by this product. Clarification for objects contained in this table as it applies to the FrameSaver access unit is provided below.

| Object | Description | Setting/Contents |
|---|---|---|
| frCircuitDlci *(frCircuitEntry 2)* | Contains the DLCI number for a virtual circuit on the frame relay interface. Only DLCIs with a configured DLCI record are supported. Supported as an index and a read-only value. | Corresponds to the DLCI Number configuration option (range 16 to 1007). |
| frCircuitState *(frCircuitEntry 3)* | Indicates whether the particular virtual circuit is operational.<br>This object can only be used to place a circuit in or out of service. It cannot be used to add or delete a circuit. | Indicates a DLCI's configured state if LMI Personality is set to None and a "get" is performed.<br>Changes how a DLCI is configured based upon whether a "get" or "set" is performed.<br>Supports only the following values:<br>■ **active(2)** – Indicates that the DLCI is active and enabled and can be used for transfer of information on the frame relay interface.<br>■ **inactive(3)** – Indicates that the DLCI is inactive or disabled and cannot be used for transfer of information on the frame relay interface. |

| Object | Description | Setting/Contents |
|---|---|---|
| Circuit Statistics *(frCircuit Entry 4 to 9)* | Contains the statistics for a particular circuit. These statistics manage the SNMP Managers to which the access unit reports traps. Statistics are kept since the last Statistics Clear command was issued by the user, or since the circuit was created if a clear has never been issued. | The MIB objects and their corresponding statistics are:<br>■ frCircuitReceivedFECNs (*frDlcmiEntry 4*) – FECNs Received statistic<br>■ frCircuitReceivedBECNs (*frDlcmiEntry 5*) – BECNs Received<br>■ frCircuitSentFrames (*frDlcmiEntry 6*) – Frames Sent statistic<br>■ frCircuitSentOctets (*frDlcmiEntry 7*) – Characters Sent statistic<br>■ frCircuitReceivedFrames (*frDlcmiEntry 8*) – Frames Received<br>■ frCircuitReceivedOctets (*frDlcmiEntry 9*) – Characters Received |
| frCircuitCommitted Burst *(frCircuit Entry 12)* | Indicates the maximum amount of data (in bits) that the network agrees to transfer under normal conditions during the measurement interval. | Corresponds to the Committed Information Rate (CIR). |
| frCircuitExcess Burst *(frCircuitEntry 13)* | Indicates the maximum amount of uncommitted data bits that the network will attempt to deliver over the measurement interval (interval = 1 second). | Corresponds to the Excess Burst Size (Bits) configuration option. |
| frCircuit Throughput *(frCircuitEntry 14)* | Indicates the average number of bits per second of frame relay information transferred across the network interface in one direction, measured over the measurement interval. | Read only |

## Error Group

The Error Group consists of the Error Table, which contains an entry for each frame relay interface that describes errors found on each interface. Clarification for objects contained in this table as it applies to the FrameSaver access unit is provided below.

| Object | Description | Setting/Contents |
|---|---|---|
| frErrType<br>*(frErrEntry 2)* | Indicates the type of error that was last seen on this frame relay interface. | Supports only the following values:<br>■ unknownError(1)<br>■ receiveShort(2)<br>■ receiveLong(3)<br>■ illegalDLCI(4)<br>■ unknownDLCI(5)<br>■ dlcmiProtoErr(6)<br>■ dlcmiUnknownIE(7)<br>■ dlcmiSequenceErr(8)<br>■ noErrorSinceReset(10) |
| frErrData<br>*(frErrEntry 3)* | Contains an octet string up to 4 bytes long. This string represents the first 4 bytes of the last frame that was in error. | Octet string |

## Global Objects

The global objects are:

- Frame Relay Trap State – Not supported. The value is always noSuchName.
- DLCI Status Change Trap – Not supported.

# Frame Relay Service MIB, RFC 1604

The frameRelayService object defined by RFC 1604 is supported for both the Network and the synchronous data ports when the interface is configured to support the service side of the frame relay UNI. An interface is considered to support the service side when the LMI Personality configuration option is set to Network Side. RFC 1604 is an SNMPv2 MIB, but is converted to an SNMPv1 MIB to support this access unit.

The Frame Relay Service MIB consists of seven groups and one object:

- Logical Port Group
- Management VC Signaling Group
- PVC End-Point Group
- PVC Connection Group – Not supported.
- Accounting Group – Not supported.
- frPVCConnectIndex Value Object – Not supported.
- frNetServObjects Group – Limited support.
- frNetServTraps Group – Not supported.

## Logical Port Group

The Logical Port Group consists of the Frame Relay Port Information table. Clarification for objects contained in this table as it applies to the FrameSaver access unit is provided below.

| Object | Description | Setting/Contents |
|---|---|---|
| frLportNumPlan *(frLportrEntry 1)* | Identifies the network address number plan for the UNI/NNI logical port. | Supports only the following value:<br>■ **none(4**) – The SNMP agent will return an octet string of zero length for the ifPhysAddress. |
| frLportContact *(frLportEntry 2)* | Identifies the network contact for this UNI port. | The access unit does not support a different contact per interface. The value for this object is the information contained in the System Contact object of MIB II. |
| frLportLocation *(frLportrEntry 3)* | Identifies the frame relay network location for this UNI frame relay interface. | The access unit does not support a different location per interface. The value for this object is the information contained in the System Location object of MIB II. |
| frLportType *(frLportrEntry 4)* | Identifies the type of network interface for this frame relay interface. | Since this access unit does not support a network-to-network interface (NNI), only the following value is supported:<br>■ **uni(1**) – The frame relay interface supports the service side of the user-to-network interface (UNI). |
| frLportAddrDLCI Len *(frLportrEntry 5)* | Identifies the Q.922 address field length and the DLCI length for this frame relay interface. | Supports only the following value:<br>■ **twoOctets10Bits(1**) – The frame relay address field length is two octets, and the DLCI is 10 bits. |
| frLportVCSig Protocol *(frLportrEntry 6)* | Identifies the local in-channel signaling protocol that is used for this frame relay interface. The value corresponds to the LMI Protocol configuration option. | The values supported are:<br>■ **none(1**) – No LMI is supported on this interface.<br>■ **lmi(2)** – The standard LMI is supported on this interface.<br>■ **ansiT1617D(3)** – The LMI supported on this interface complies with ANSI T1.617, Annex D.<br>■ **ccittQ933A(5)** – The LMI supported on this interface complies with CCITT Q.933, Annex A. |

## Management VC Signaling Group

The Management VC Signaling Group consists of the Frame Relay Management VC Signaling Table. Clarification for objects contained in this table as it applies to the FrameSaver access unit is provided below.

| Object | Description | Setting/Contents |
|---|---|---|
| frMgtVCSigProced *(frMgtVCSig Entry 1)* | Identifies the local in-channel signaling procedure used for this frame relay interface. | Supports only the following value:<br>■ **u2nnet(1**) – Only the user-to-network, service side procedures are performed. |
| DTE-Side LMI Parameters | DTE side protocol parameters are not supported since this MIB is only supported for service-side LMI. | The value of the following MIB objects is equal to **NoSuchName:**<br>■ frMgtVCSigUserN391 (*frMgtVCSigEntry 2*)<br>■ frMgtVCSigUserN392 (*frMgtVCSigEntry 3*)<br>■ frMgtVCSigUserN393 (*frMgtVCSigEntry 4*)<br>■ frMgtVCSigUserT391 (*frMgtVCSigEntry 5*) |
| Service-Side LMI Parameters | Identify the service-side protocol parameters that control the operation of the LMI link for the frame relay interface. | The values of the objects are:<br>■ frMgtVCSigNetN392 (*frMgtVCSigEntry 6*) – LMI Error Event(N2) configuration option<br>■ frMgtVCSigNetN393 (*frMgtVCSigEntry 7*) – LMI Clearing Events (N3) configuration option<br>■ frMgtVCSigNetT392 (*frMgtVCSigEntry 8*) – LMI Inbound Heartbeat (T2) configuration option<br>■ frMgtVCSigNetnN4 (*frMgtVCSigEntry 9*) – LMI Max Network Status Enquiries (N4) configuration option<br>■ frMgtVCSignetT3 (*frMgtVCSigEntry 10*) – LMI N4 measurement Period (T3) configuration option |

| Object | Description | Setting/Contents |
|---|---|---|
| DTE-Side Error Statistics | Do not support DTE side error statistics since this MIB is only supported for service-side LMI. | The value of the following MIB objects is equal to **NoSuchName:**<br>■ frMgtVCSigUserLinkRelErrors (*frMgtVCSigEntry 11*)<br>■ frMgtVCSigUserprotErrors (*frMgtVCSigEntry 12*)<br>■ frMgtVCSigUserChanInactive (*frMgtVCSigEntry 13*) |
| Service-Side Error Statistics | Contain the error statistics for a particular circuit. These statistics are kept since the last Statistics Clear command has been issued by the user, or since the circuit was created if a clear has never been issued. | The values of the objects are:<br>■ frMgtVCSigNetLinkRelErrors (*frMgtVCSigEntry 14*) – Reliability Errors statistic<br>■ frMgtVCSigNetProtErrors (*frMgtVCSigEntry 15*) – Protocol Errors statistic<br>■ frMgtVCSigNetChanInactive (*frMgtVCSigEntry 16*) – Number of Inactives statistic |

## PVC End-Point Group

The PVC End-Point Group consists of the PVC End-Point Table, which contains an entry for each virtual circuit (identified by DLCI number) supported on a specific frame relay interface (identified by ifIndex). This table contains an entry for a specific DLCI only when a DLCI record has been created for it. Creation and deletion of DLCIs through the circuit table is not supported by the FrameSaver access unit.

All objects in this table are treated as read-only by the FrameSaver access unit, unless otherwise specified. Clarification for objects contained in this table as it applies to the access unit is provided below.

| Object | Description | Setting/Contents |
|---|---|---|
| frPVCEndPtDLCI Index *(frPVCEndpt Entry 1)* | Contains the DLCI number for the virtual circuit on the frame relay interface.<br>This is a nonaccessible index; a “getnext” must be used to obtain the first object supported. With a returned OID, “getnext” can be used for the rest of the objects. A “get’’ only returns the first object. | Corresponds to the DLCI configuration option and can range from **16** to **1007**. |
| Max Frame Size Objects | Two MIB objects are supported, one for ingress into the frame relay network and one for egress. | Supports only a single frame size for both directions, so the following objects contain the same value of **2048**:<br>■ frPVCEndptInMaxFrameSize (*frPVCEndptEntry 2*)<br>■ frPVCEndptOutmaxFrame Size (*frPVCEndptEntry 6*) |
| Committed Burst Size Objects | Two MIB objects are supported, one for ingress into the frame relay network and one for egress. | Supports only a single committed burst size for both directions, so both objects will contain the same value. The objects are:<br>■ frPVCEndptInBc (*frPVCEndptEntry 3*)<br>■ frPVCEndptOutBc (*frPVCEndptEntry 7*) |
| Excess Burst Size Objects | There are two MIB objects for excess burst size, one for ingress into the frame relay network and one for egress direction. | Indicates the maximum amount of uncommitted data bits that the network will attempt to deliver over the measured interval of 1 second. The value of the following objects are:<br>■ frPVCEndptInBe (*frPVCEndptEntry 4*)<br>■ frPVCEndptOutBe (*frPVCEndptEntry 8*) |

| Object | Description | Setting/Contents |
|---|---|---|
| Committed Information Rate Objects | There are two MIB objects for Committed Information rate (CIR), one for ingress into the frame relay network and one for egress. | Supports only a single CIR for both directions, so the following objects contain the same value which corresponds to the CIR configuration option:<br>■ frPVCEndptInCIR (*frPVCEndptEntry 5*)<br>■ frPVCEndptOutCIR (*frPVCEndptEntry 9*) |
| frPVCEndpt Connect Identifier *(frPVCEndpt Entry 10)* | Identifies PVC endpoints as being one part of a PVC connection. This object is an index into the PVC Connection Table, which is not supported by the access unit. | The value of this MIB object is **noSuchName.** |
| frPVCEndptRow Status *(frPVCEndpt Entry 11)* | Creates, modifies and deletes rows in the PVC Connection Table. These operations are not supported by the access unit. | The value of this MIB object is **noSuchName.** |
| frPVCEndptRcvd SigStatus *(frPVCEndpt Entry 12)* | Identifies the status received via the local in-channel signaling procedures for this PVC endpoint. | Supports only the following value:<br>■ **none(4)** – Only choice available when network-side procedures are being performed. |

| Object | Description | Setting/Contents |
|---|---|---|
| Circuit Statistics *(frPVCEndpt Entry 13–20)* | Contain the statistics for a particular circuit. These statistics are kept since the last Statistics Clear command has been issued by the user, or since the circuit was created if a clear has never been issued. | The MIB objects and their corresponding statistics are:<br>■ frPVCEndptInFrames (*frPVCEndptEntry 13*) – Frames Received statistic<br>■ frPVCEndptOutFrames (*frPVCEndptEntry 14*) – Frames Sent statistic<br>■ frPVCEndptInOctets (*frPVCEndptEntry 19*) – Characters Received statistic<br>■ frPVCEndptOutOctets (*frPVCEndptEntry 20*) – Characters Sent statistic<br><br>Supported MIB objects that do not have corresponding statistics are:<br>■ frPVCEndptInExcessFrames (*frPVCEndptEntry 16*)<br>■ frPVCEndptOutExcess Frames (*frPVCEndptEntry 17*)<br><br>MIB objects not supported and that return a zero value are:<br>■ frPVCEndptInDEFrames (*frPVCEndptEntry 15*)<br>■ frPVCEndptInDiscards (*frPVCEndptEntry 18*) |

## PVC Connection Group

The Frame Relay PVC Connection Status Change trap (frPVCConnectStatusChange) is not supported.

# RS-232-Like MIB, RFC 1659

Supported for all of the synchronous data ports and for the COM port. RFC 1659 is an SNMPv2 MIB, but is converted to an SNMPv1 MIB to support this access unit. One object, five tables, and one group are supported for this MIB:

- Number of RS-232-Like Ports
- General Port Table
- Asynchronous Port Table – Not supported for the synchronous data ports.
- Synchronous Port Table
- Input Signal Table – Not supported for the COM port.
- Output Signal Table – Not supported for the COM port.
- Conformance Group – Not supported

## Number of RS-232-Like Ports

Supported as documented in the RFC. The number of ports is set to three: two data ports and one COM port.

## General Port Table

The General Port Table contains configuration options for the RS-232-Like interfaces. Clarification for objects contained in this table as it applies to the FrameSaver access unit is provided below.

| Object | Description | Setting/Contents |
|---|---|---|
| rs232PortType *(rs232PortEntry 2)* | Identifies the port hardware type. | Supports only the following values:<br>■ **rs232(2)** – Identifies the COM port, or the synchronous ports configured as EIA-232.<br>■ **v35(5)** – Identifies the synchronous ports configured as V.35. |
| rs232PortInSig Number *(rs232PortEntry 3)* | Contains the number of input signals in the input signal table. | The value is **2** for synchronous ports and **0** for the COM port. |
| rs232PortOutSig Number *(rs232PortEntry 4)* | Contains the number of output signals in the output signal table. | The value is **2** for synchronous ports and **0** for the COM port. |

| Object | Description | Setting/Contents |
|---|---|---|
| rs232PortInSpeed *(rs232PortEntry 5)* | Contains the port's input speed in bits per second. | Supports the following speeds for the data ports: 4800, 9600, 14,400, 16,800, 19,200, 24,000, 28,800, 38,400, 48,000, 56,000, 64,000, 128,000, 192,000, 256,000.<br>Speeds available for the COM port: 9600, 14,400, 19,200, 28,800, 38,400, 57,600, and 115,200. |
| rs232PortOut Speed *(rs232PortEntry 6)* | Contains the port's output speed in bits per second. | Same as rs232PortInSpeed. |
| rs232PortInFlow Type *(rs232PortEntry 7)* | Contains the port's type of input flow control. | Supports the following values:<br>■ **none(1)** – No flow control.<br>■ **ctsRts(2)** – Indicates that CTS is being used for flow control. Also indicates that both CTS and DTR are being used for flow control.<br>■ **dsrDTR(3)** – Only DTR is being used for flow control.<br>**NOTE:** The above settings are mutually exclusive. There is no way to set the value "Both", to ignore both control leads. If "Both" is the current setting in the unit, the value returned for this object is ctsRts(2). |
| rs232PortOutFlow Type *(rs232PortEntry 8)* | Contains the port's type of output flow control. | Supports only the following value:<br>■ **none(1)** – No flow control. |

## Asynchronous Port Table

The Asynchronous Port Table contains an entry for the COM port when the port is configured for asynchronous operation. The Asynchronous Port Table is not supported for the synchronous data ports. This object is supported for the COM port only. For this access unit, entries in the table that are counters (rs232AsyncPortEntry 6 to 8) are used to collect statistics only and are not supported. Clarification for objects contained in this table as it applies to the access unit is provided below.

| Object | Description | Setting/Contents |
|---|---|---|
| rs232AsyncPort Bits *(rs232Async PortEntry 2)* | Specifies the number of bits in a character. | Supports only the following values:<br>■ **7** – 7-bit characters<br>■ **8** – 8-bit characters |
| rs232AsyncPort StopBits *(rs232Async PortEntry 3)* | Specifies the number of stop bits supported. | Supports only the following values:<br>■ **one(1)** – One stop bit<br>■ **two(2)** – Two stop bits |
| rs232AsyncPort Parity (*rs232Async PortEntry 4)* | Specifies the type of parity used by the port. | Supports only the following values:<br>■ **none(1)** – No parity bit<br>■ **odd(2)** – Odd parity<br>■ **even(3)** – Even parity |
| rs232AsyncPort AutoBaud *(rs232Async PortEntry 5)* | Specifies the ability to automatically sense the input speed of the port. | Supports only the following value:<br>■ **disabled(2)** – Does not support Autobaud. |

## Synchronous Port Table

The Synchronous Port Table contains an entry for each of the synchronous data ports and the COM port when the port is configured for synchronous operation. For this access unit, entries in the table that are counters (rs232SyncPortEntry 3 to 7) are used to collect statistics only and are not supported.

Clarification for objects contained in this table as it applies to the FrameSaver access unit is provided below.

| Object | Description | Setting/Contents |
|---|---|---|
| rs232SyncPort ClockSource *(rs232Sync PortEntry 2)* | Specifies the clock source for the port. | Supports only the following values:<br>■ **internal(1)** – The port uses an internal clock.<br>■ **external(2)** – The port uses an external clock. |
| rs232SyncPort Role *(rs232Sync PortEntry 8)* | Specifies whether this device interface is a DTE or DCE. | Supports only the following value:<br>■ **dce(2)** – The port acts as a DCE. |
| rs232SyncPort Encoding *(rs232Sync PortEntry 9)* | Specifies the bit encoding technique that this port uses. | Supports only the following value:<br>■ **nrz(1)** – The port uses non-return to zero encoding. |
| rs232SyncPort RTSControl *(rs232Sync PortEntry 10)* | Specifies the method used to control the RTS signal. | Supports only the following values:<br>■ **controlled(1)** – For user data ports, this value is used when the port is configured for RTS or Both.<br>■ **constant(2)** – For user data ports, this value is used when the port is configured for DTR or None. This is the only valid value for the COM port. |
| rs232SyncPort RTSCTSDelay *(rs232Sync PortEntry 11)* | Specifies the interval (in milliseconds) that the DTE must wait after RTS is asserted before it can assert CTS. | Supports only the following value:<br>■ **0** – The port does not have to wait. |
| rs232SyncPort Mode *(rs232Sync PortEntry 12)* | Specifies the port's mode of operation with respect to the direction and simultaneousness of the data transfer. | Supports only the following value:<br>■ **fdx** – full duplex |

| Object | Description | Setting/Contents |
|---|---|---|
| rs232SyncPortIdle Pattern *(rs232Sync PortEntry 13)* | Specifies the bit pattern used to indicate an idle line. | This MIB object is not supported since flags (xFE) are used as IDLE and the only choices in the MIB are mark and space. |
| rs232SyncPort MinFlags *(rs232Sync PortEntry 14)* | Specifies the minimum number of flag patterns the port needs to recognize the end of one frame and the start of another. | Supports only the following value:<br>■ **2** – The minimum number of flags supported for all ports on the access unit. |

## Input Signal Table

The Input Signal Table contains entries for the input signals that can be detected by the FrameSaver access unit for each of the synchronous data ports. Clarification for objects contained in this table as it applies to the FrameSaver access unit is provided below.

| Object | Description | Setting/Contents |
|---|---|---|
| rs232InSigName *(rs232InSig Entry 2)* | Contains the ID of a hardware input signal. | Supports only the following values:<br>■ **rts(1)** – Request To Send<br>■ **dtr(4)** – Data Terminal Ready |
| rs232InSigState *(rs232InSig Entry 3)* | Contains the current signal state. | Supports only the following values:<br>■ **on(2)** – The signal is asserted.<br>■ **off(3)** – The signal is de-asserted. |
| rs232InSig Changes *(rs232InSig Entry 4)* | Indicates the number of times that a signal has changed from on to off, or off to on. | Not supported. |

## Output Signal Table

The Output Signal Table contains entries for the output signals that can be asserted by the FrameSaver access unit for each of the synchronous data ports. Clarification for objects contained in this table as it applies to the FrameSaver access unit is provided below.

| Object | Description | Setting/Contents |
|---|---|---|
| rs232OutSigName *(rs232OutSig Entry 2)* | Contains the ID of a hardware output signal. | Supports only the following values:<br>■ **cts(2)** – Clear To Send<br>■ **dsr(3)** – Data Set Ready |
| rs232OutSigState *(rs232OutSig Entry 3)* | Contains the current signal state. | Supports only the following values:<br>■ **on(2)** – The signal is asserted.<br>■ **off(3)** – The signal is deasserted. |
| rs232OutSig Changes *(rs232OutSig Entry 4)* | Indicates the number of times that a signal has changed from on to off, or off to on. | Not supported. |

# Enterprise MIB

The following lists the enterprise-specific MIB objects supported by the unit:

- Device Configuration MIB
- Port Usage Table
- DDS Interface-Specific Definitions
- Device Security Table
- Device Traps Table
- Device Control Object
- Device Health and Status Object
- Frame Relay PVC Cross Connect Table
- Frame Relay PVC Test Group
- Frame Relay Clear Statistics Group
- Frame Relay Extension Group
- Data Compression Group
- IP Route Table

## Device Configuration MIB, devConfig (*ID*-common 7)

The variable devConfigAreaCopy under the devConfigArea group (devConfig.mib) is supported. This variable allows the entire contents of one configuration area to be copied into another configuration area. The FrameSaver access unit only supports the following values:

| Object | Description | Setting/Contents |
|---|---|---|
| devConfigArea Copy | A “get” of this object will always return noOp. | noOp(1) |
| | Copy from active area to customer 1 area. | active-to-customer1(2) |
| | Copy from active area to customer 2 area. | active-to-customer2(3) |
| | Copy from customer 1 area to active area. | customer1-to-active(4) |
| | Copy from customer 1 area to customer 2 area. | customer1-to-customer2(5) |
| | Copy from customer 2 area to active area. | customer2-to-active(6) |
| | Copy from customer 2 area to customer 1 area. | customer2-to-customer1(7) |
| | Copy from factory area to active area. | factory1-to-active(8) |
| | Copy from factory area to customer 1 area. | factory1-to-customer1(9) |
| | Copy from factory area to customer 2 area. | factory1-to-customer2(10) |

## Port Usage Table, devPortUsage (*ID*-interfaces 3)

The Port Usage table (devPortUsage.mib) specifies whether the COM port is configured for the asynchronous terminal interface, ASCII alarms, or as an SNMP management link.

The value **other(4)** is not supported for the COM port.

## DDS Interface-Specific Definitions, dds (*ID*-interfaces 2)

The DDS Interface Specific Definitions contain objects that are used to manage the DDS Network Interface. All of these objects are supported by the FrameSaver access unit, except as described below:

| Object | Description | Setting/Contents |
|---|---|---|
| **DDS Status Table** | | |
| ddsAlarmStatus *(ddsStatusEntry 4)* | A bitmap represented as a sum, which can represent multiple conditions simultaneously.<br>It is used to view current alarm conditions. | Supports only the following conditions:<br>■ 1 – operational<br>■ 2 – crossPairDetected<br>■ 4 – noSignal<br>■ 8 – outOfService<br>■ 16 – outOfFrame<br>■ 32 – excessiveBPVs |
| ddsClearChannel DataScrambling *(ddsConfigEntry 3)* | Controls whether data scrambling is used. This is to prevent Latching Loopbacks caused by application data. | Not supported. |
| ddsInBandManagementChannel *(ddsConfigEntry 4)* | Configures the speed of the proprietary in-band managment channel. | Not supported. |
| ddsInBandFramingErrorAlarm *(ddsConfigEntry 9)* | Controls whether an ASCII alarm is generated when in-band framing errors occur. | Not supported. |

| Object | Description | Setting/Contents |
|---|---|---|
| **DDS Test Table** | | |
| ddsTestStatus *(ddsTestEntry 2)* | A bitmap represented as a sum, which can represent multiple conditions simultaneously.<br>It is used to view the status of currently-running tests. | Supports only the following conditions:<br>■ 1 – csuLoopback<br>■ 2 – dsuLoopback<br>■ 8 – nonLatchingCSULoopback<br>■ 16 – nonLatchingDSULoopback<br>■ 32 – sending511Pattern<br>■ 64 – monitoring511Pattern |
| ddsTestStart *(ddsTestEntry 3)* | A bitmap represented as a sum, which can represent multiple conditions simultaneously.<br>It is used to start specific tests. | Supports only the following conditions:<br>■ 1 – csuLoopback<br>■ 2 – dsuLoopback<br>■ 16 – send511<br>■ 32 – monitor511 |
| ddsTestStop *(ddsTestEntry 4)* | A bitmap represented as a sum, which can represent multiple conditions simultaneously.<br>It is used to stop specific tests. | Performing a “get” always yields 0.<br>Supports only the following conditions:<br>■ 1 – csuLoopback<br>■ 2 – dsuLoopback<br>■ 4 – send511<br>■ 8 – monitor511 |
| ddsTestCode *(ddsTestEntry 5)* | A read-only code containing more specific information concerning test pattern monitoring results. | Supports the following conditions:<br>■ **none(1)** – No monitor tests are running or no further information is available.<br>■ **inSyncNoBitErrors(2)** – Monitor pattern test has synchronized without bit errors.<br>■ **inSyncWithBitErrors(3)** – Monitor pattern test has synchronized with bit errors.<br>■ **notInSync(4)** – Monitor pattern test has not synchronized. |
| ddsTestErrorCount *(ddsTestEntry 6)* | Indicates the number of errors detected while monitoring a pattern test. | Value between **0** and **99,999**. |

### Device Security Table, *ID*-security (*ID*-common 8)

The Device Security Table (devSecurity.mib) controls the number of SNMP Managers that may access the access unit, as well as the access level (read or read/write). This table is fully supported except for the new security manager table (newSecurityMgrTable), which is not supported.

### Device Traps Table, *ID*-traps (*ID*-common 9)

The Device Traps Table (devTrapMgr.mib) manages the SNMP Managers to which the access unit reports traps. This table is fully supported.

### Device Control Object, *ID*-control (*ID*-common 10)

The devControlReset (devControl.mib) object resets the device using the devControlReset (devControl.mib) object, and performs a lamp test. This object is fully supported.

### Device Health and Status Object, devStatus (*ID*-devStatus 1)

The devStatus (devHealthAndStatus.mib) object reports the FrameSaver access unit's health and status and self-test result messages. This object is fully supported.

### Frame Relay PVC Cross Connect Table, pvcXconnect (crossConnect 3)

The Frame Relay PVC Cross-Connect Table (devPVCXconnect.mib) manages PVC connections. Contains a list of DLCI/EDLCI cross-connections and their addresses. Includes Alternate Destination information, if configured. This table is supported as read-only.

### Frame Relay PVC Test Group, devPVCTest (*ID*FrameRelay 3)

The Frame Relay PVC Test Group (devPVCtest.mib) is used to start and stop tests on DLCIs, as well a monitor the results of the tests. Fully supported except that the devPVCActiveTestDisruptive object is supported as read-only.

### Frame Relay Clear Statistics Group, frame-relay-clear-stat (*ID*FrameRelay 1)

The frame-relay-clear-stat group is used to clear statistics that are provided in the standard Frame Relay MIBs, as well as the LMI and DLCI statistics. This object is fully supported.

## Frame Relay Extension Group, devFrExt (*ID*FrameRelay 4)

The frame-relay extension group contains extensions to the RFC 1315 and RFC 1604 MIBs that provide additional configuration options and statistics. This object is fully supported.

## Frame Relay Data Compression Group, frNetDcp (*ID*FrameRelay 2)

The frNetDcp group (frNetDcp.mib) is used to enable management of the Frame Relay Forum's implementation agreements for data compression (FRF.9). This group is fully supported with the following exceptions:

| Object | Description | Setting/Contents |
|---|---|---|
| frDcpPortFlow Control (*frDcpPortEntry 3*) | Indicates how data compression should occur. | All items but **clock clamp(3)** are fully supported. |
| frDcpDlciTable (*frNetDcp 2*) | Contains all data compression status and statistical information for a port or DLCI.<br>Allows:<br>■ Clearing of data compression statistics for a port or DLCI.<br>■ Enabling/disabling compression for a DLCI. | All objects but the following are supported:<br>■ frDcpRxThrPut (*frDcpDlciEntry 8*)<br>■ frDcpStatsClearAll (*frDcpDlciEntry 12*) |

## IP Route Table, devIPRouteTable (*ID*-ip 1)

The IP routing table (devIPRoute.mib) is used to manage IP routes. All routes appear on this table and are fully supported with the following exceptions:

| Object | Description | Setting/Contents |
|---|---|---|
| ipRouteType *(devIPRoute Entry 8)* | Can be used to delete an IP route. | Set its value to **invalid(2)** to delete an IP route. |
| ipRouteAge *(devIPRoute Entry 10)* | Reflects the value of the time-to-live for the route (in seconds). | Supported as read-only. |

# Standards Compliance for SNMP Traps

# D

This appendix describes the FrameSaver access unit's compliance with SNMP format standards and with its special operational trap features. The FrameSaver access unit supports the following user interface traps, along with several enterprise-specific traps:

- warmStart
- authenticationFailure
- linkUp
- linkDown

These traps are listed in alphabetical order within each table.

## Trap: warmStart

| Trap | What It Indicates | Possible Cause |
|---|---|---|
| warmStart | Access unit has just reinitialized and stabilized itself. | ■ Reset command sent.<br>■ Power disruption. |

# Trap: authenticationFailure

| Trap | What It Indicates | Possible Cause |
|---|---|---|
| authenticationFailure | Access to the access unit was attempted and failed. | ■ SNMP protocol message not properly authenticated.<br>■ Three unsuccessful attempts were made to enter a correct login/password combination.<br>■ IP address security is enabled, and a message was received from SNMP Manager whose address was not on the list of approved managers. |

# Traps: linkUp and linkDown

| Trap | What It Indicates | Possible Cause |
|---|---|---|
| linkDown | A failure in one of the communication interfaces has occurred. | A failure in one of the communication interfaces has occurred. |
| linkUp | One of the failed communication interfaces is up and operational. | One of the failed communication interfaces is up and operational. |

The interfaces that support these traps and conditions that define linkUp and linkDown for each interface include the following:

| Interface | linkUp/Down Variable-Bindings | Possible Cause |
|---|---|---|
| **Physical Sublayer** – Represented by the entry in the MIB II Interfaces Table. | | |
| DDS Network<br>(Supported by the media-specific DDS Enterprise MIB.) | ■ ifIndex (RFC 1573)<br>■ ifAdminStatus (RFC 1573)<br>■ ifOperStatus (RFC 1573)<br>■ ifType (RFC 1573)<br>■ ddsStatus (DDS Enterprise MIB) | ■ linkDown – One or more alarm conditions are active on the interface.<br>Alarm conditions include:<br>– No Signal<br>– Out of Service<br>– Out of Frame<br>– Crossed Pair Detected<br>– Excessive Bipolar Violations (BPVs)<br>■ linkUp – No alarms on the interface. |
| Synchronous Data Ports<br>(Supported by the media-specific RS232-like MIB.) | ■ ifIndex (RFC 1573)<br>■ ifAdminStatus (RFC 1573)<br>■ ifOperStatus (RFC 1573)<br>■ ifType (RFC 1573) | ■ linkDown – One or more alarm conditions are active on the port.<br>Alarm conditions include:<br>– DTR Off [1]<br>– RTS Off [2]<br>– Compression Connection Failure<br>– Low Compression Ratio<br>■ linkUp – No alarms on the port. |
| Network Communication Link (COM Port)<br>(Supported by the media-specific RS232-like MIB.) | ■ ifIndex (RFC 1573)<br>■ ifAdminStatus (RFC 1573)<br>■ ifOperStatus (RFC 1573)<br>■ ifType (RFC 1573) | ■ linkDown – One or more alarm conditions are active on the port.<br>Alarm conditions include:<br>– DTR Off [1]<br>– RTS Off [2]<br>– Compression Connection Failure<br>– Low Compression Ratio<br>■ linkUp – No alarms on the port. |
| [1] The DTR alarm condition will only generate a linkUp/linkDown trap if the DTE supports the DTR lead state.<br>[2] The RTS alarm condition will only generate a linkUp/linkDown trap if the DTE supports the RTS lead state. | | |

| Interface | linkUp/Down Variable-Bindings | Possible Cause |
|---|---|---|
| **Logical Link Sublayer** – Represented by the entry in the MIB II Interfaces Table. | | |
| Service Side of the Frame Relay UNI<br>(Supported by the media-specific Frame Relay Services MIB.) | ■ ifIndex (RFC 1573)<br>■ ifAdminStatus (RFC 1573)<br>■ ifOperStatus (RFC 1573)<br>■ ifType (RFC 1573)<br>■ frLportVCSigProtocol (Frame Relay Services MIB)<br>■ frMgtVCSigNetChan-Inactive (Frame Relay Services MIB) | ■ linkDown – LMI is down for the LMI Protocol configured,[3] or Frame Relay link is disabled.<br>■ linkUp – LMI is up or Frame Relay link is enabled. |
| DTE Side of the Frame Relay UNI<br>(Supported by the media-specific Frame Relay DTE's MIB.) | ■ ifIndex (RFC 1573)<br>■ ifAdminStatus (RFC 1573)<br>■ ifOperStatus (RFC 1573)<br>■ ifType (RFC 1573)<br>■ frDlciState (Frame Relay DTEs MIB) | ■ linkDown – LMI is down for the LMI Protocol configured,[3] or Frame Relay link is disabled.<br>■ linkUp – LMI is up or Frame Relay link is enabled. |

[3] If the LMI Protocol is not configured, a linkUp/linkDown trap is based solely upon whether the interface is enabled or disabled.

# Traps: enterprise-Specific

These traps indicate that an enterprise-specific event has occurred. Supported enterprise-specific traps include the following, listed in alphabetical order:

| Trap | What It Indicates | Possible Cause |
|---|---|---|
| enterpriseConfig Change(6) | Configuration has been changed via the user interface or an SNMP Manager after 60 seconds has elapsed without another change.<br>This trap does not have a variable binding. | Configuration has been changed via the user interface or an SNMP Manager. |
| enterpriseDevice Fail(3) | An internal device failure.<br>This trap does not have a variable binding. | Operating software has detected an internal device failure. |
| enterpriseDLCInet UNIDown(11) | The DLCI for an interface supporting the Service Side of the UNI is down. | DLCI is down. |
| enterpriseDLCInet UNIUp(12) | The DLCI for an interface supporting the Service Side of the UNI is up. | DLCI is up again. |
| enterpriseLow CompressionRatio(10) | The compression ratio has dropped below the specified threshold. | DLCI Compression Ratio Threshold for Port-1 was set too high. |
| enterpriseLow CompressionRatio Clear(110) | The compression ratio has risen above the specified threshold. | DLCI Compression Ratio Threshold for Port-1 was set too low. |
| enterpriseSelfTest Fail(2) | A hardware failure.<br>The variable binding for this trap is devSelfTestResults. | Unit has completed (re)initialization and a hardware failure was detected. |
| enterpriseTest Start(5) | A test is running. | At least one test has been started on an interface or virtual circuit. |
| enterpriseTest Stop(105) | All tests have been halted. | All tests have been halted on an interface or virtual circuit. |

Tests that affect the enterpriseTestStart and enterpriseTestStop traps and variable-bindings are different for each interface. The tests that support these traps and their variable-bindings include the following:

| Interface | enterpriseTestStart/Stop Variable-Bindings | Possible Cause |
|---|---|---|
| **Physical Sublayer** | | |
| DDS Network | ■ ifIndex (RFC 1573)<br>■ ifAdminStatus (RFC 1573)<br>■ ifOperStatus (RFC 1573)<br>■ ifType (RFC 1573)<br>■ ddsTestStatus (DDS Enterprise MIB) | ■ enterpriseTest Start – The following tests are active on the interface:<br>– DSU Loopback<br>– CSU Loopback<br>– Send 511 pattern<br>– Monitor 511 pattern<br>■ enterpriseTest Stop – No longer any tests running on the interface. |
| Synchronous Data Ports | ■ ifIndex (RFC 1573)<br>■ ifAdminStatus (RFC 1573)<br>■ ifOperStatus (RFC 1573)<br>■ ifType (RFC 1573)<br>■ ifTestType (RFC 1573) | ■ enterpriseTest Start – Any of the following tests is active on the port:<br>– DTE External Loopback<br>– Send 511 pattern<br>– Monitor 511 pattern<br>■ enterpriseTest Stop – No longer any tests running on the port. |
| **Virtual Circuits (DLCIs)** | | |
| Service Side of the Frame Relay Link | ■ ifIndex (RFC 1573)<br>■ ifAdminStatus (RFC 1573)<br>■ ifOperStatus (RFC 1573)<br>■ ifType (RFC 1573)<br>■ devPVCTestType (Enterprise MIB)<br>■ frPVCEndptDLCIIndex (Frame Relay Services MIB) | ■ enterpriseTest Start – Any of the following tests is active on the DLCI:<br>– PVC Loopback<br>– Send Pattern<br>– Monitor Pattern<br>■ enterpriseTest Stop – No longer any tests running on the port. |
| DTE Side of the Frame Relay Link | ■ ifIndex (RFC 1573)<br>■ ifAdminStatus (RFC 1573)<br>■ ifOperStatus (RFC 1573)<br>■ ifType (RFC 1573)<br>■ devPVCTestType (Enterprise MIB)<br>■ frCircuitDlci (Frame Relay DTEs MIB) | ■ enterpriseTest Start – Any of the following tests are active on the DLCI:<br>– PVC Loopback<br>– Send Pattern<br>– Monitor Pattern<br>■ enterpriseTest Stop – No longer any tests running on the port. |

Each virtual circuit on a link that supports the Service Side of the frame relay UNI is represented by an entry in the PVC End-Point Table of the Frame Relay Service MIB, supported by the enterprise-specific Frame Relay Service MIB. All virtual circuits for the frame relay link share the same entry in the MIB II Interfaces table; that is, they share the same ifIndex.

The interface that supports these traps and conditions include the following:

| **Interface** | **enterpriseDLCInetDown/Up Variable-Bindings** | **Possible Cause** |
|---|---|---|
| Service Side of the Frame Relay Link | ■ ifIndex (RFC 1573)<br>■ ifAdminStatus (RFC 1573)<br>■ ifOperStatus (RFC 1573)<br>■ ifType (RFC 1573)<br>■ frPVCEndptDLCIIndex (RFC 1604)<br>■ frPVCEndptRcvdSigStatus (RFC 1604) | ■ enterpriseDLCInetDown in service side:<br>– DLCI Status is set to Inactive.<br>– The compression connection (if compression is enabled) fails.<br>■ enterpriseDLCInetUp in service side:<br>– DLCI Status is set to active.<br>– The compression connection (if compression is enabled) is established. |
| DTE Side of the Frame Relay Link | ■ ifIndex (RFC 1573)<br>■ ifAdminStatus (RFC 1573)<br>■ ifOperStatus (RFC 1573)<br>■ ifType (RFC 1573)<br>■ frCircuitDlci (RFC 1315)<br>■ frCircuitState (RFC 1315) | ■ enterpriseDLCInetDown in service side:<br>– DLCI Status is set to Inactive.<br>– The compression connection (if compression is enabled) fails.<br>■ enterpriseDLCInetUp in service side:<br>– DLCI Status is set to active.<br>– The compression connection (if compression is enabled) is established. |

# Cables, Connectors, and Pin Assignments

# E

See the installation procedures in the *1-Slot Assembled Access Unit, Installation Instructions,* for connecting the cables.

## COM Port

The COM (communications) port connects to a PC (Personal Computer) for front panel emulation, or a VT100-compatible ASCII terminal or printer for alarms.

These cables are:

- 14-foot, 26 AWG, 8-conductor, with a non-keyed 8-position modular jack interface/connector at one end, and
- 25-pin or 9-pin connector at the other end, depending upon whether the FrameSaver access unit is connected to an async (or other VT100-compatible) terminal or a PC.

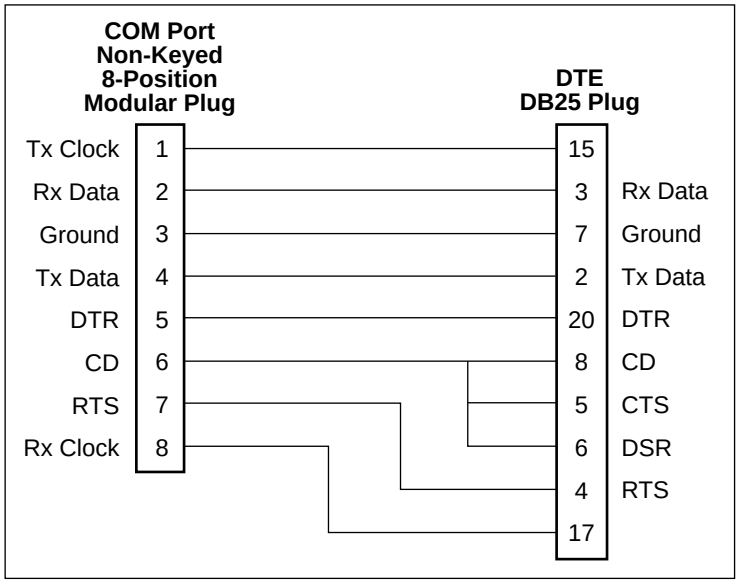
Refer to the appropriate cable section.

The following table shows the signals and pin assignments for the COM port interface/connector.

| Signal | Direction | Pin # |
|---|---|---|
| DCE Transmit Clock (TXC) | From DCE (Out) | 1 |
| DCE Received Data (RXD) | From DCE (Out) | 2 |
| Signal Ground (SG) | — | 3 |
| DCE Transmit Data (TXD) | To DCE (In) | 4 |
| DCE Data Terminal Ready (DTR) | To DCE (In) | 5 |
| DCE Carrier Detect (CD) | From DCE (Out) | 6 |
| DCE Request to Send (RTS) | To DCE (In) | 7 |
| DCE Received Clock (RXC) | From DCE (Out) | 8 |

## COM Port-to-Terminal/Printer Cable (3100-F2-540)

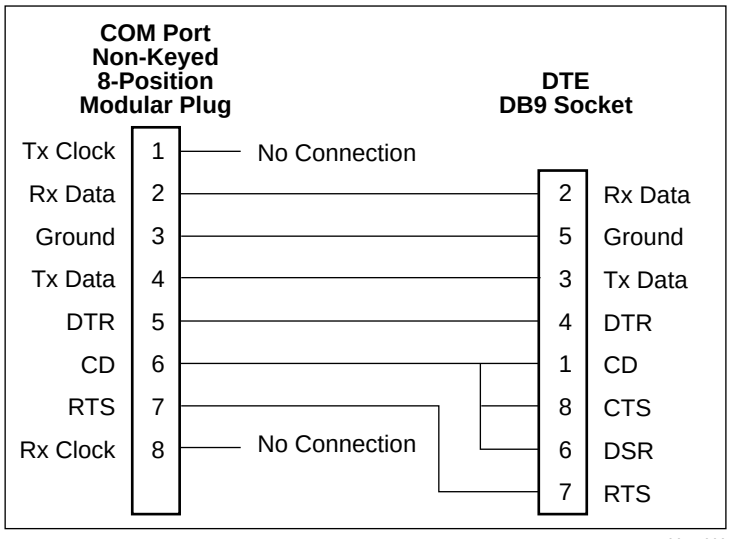
Order this cable when connecting the COM port to a terminal or printer, rather than to a PC; it does not come with the FrameSaver access unit. The following shows the pin assignments from the COM port to the terminal or printer interface.




496-14910

## COM Port-to-PC Cable (3100-F2-550)

This cable comes with the FrameSaver access unit. The following shows the pin assignments from the COM port to the PC interface.

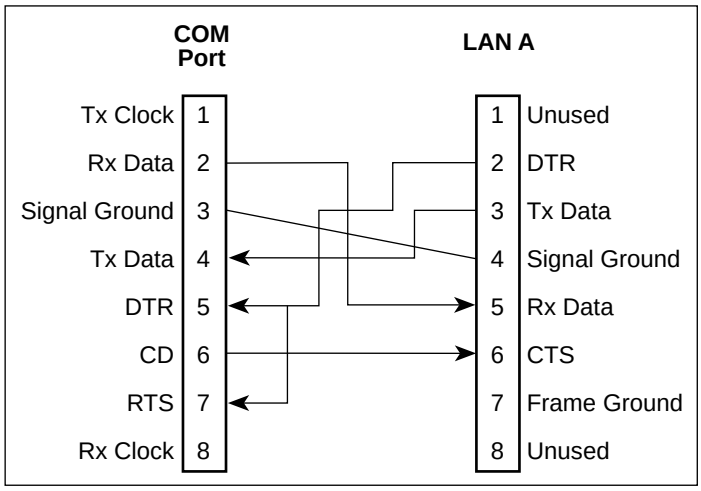



496-14909

### COM Port-to-LAN Cable (3100-F2-910)

The adapter is ordered along with the appropriate cable. Be sure to specify whether you need a Token Ring or an Ethernet cable shipped with the adapter; also specify that the interface connecting with the access unit must be unkeyed.

The following shows the pin assignments for the cable between the LAN Adapter (LAN A) and the access unit's COM port or COM Port-to-PC Adapter.




496-14908

## Modular RJ48S Network Cable

Network access is via a 14-foot modular cable with an RJ48S keyed plug-type connector on each end. The following table shows pin assignments and the purpose of each.

| Function | Circuit | Pin Number |
|---|---|---|
| Transmit ring to the local loop | R | 1 |
| Transmit tip to the local loop | T | 2 |
| Receive tip from the local loop | T1 | 7 |
| Receive ring from the local loop | R1 | 8 |

### Gender Adapter/Changer

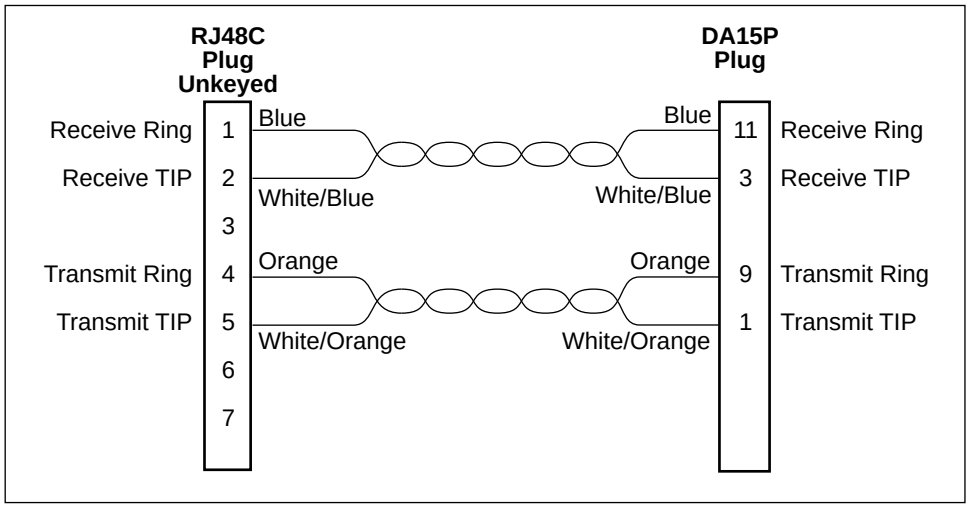
When connecting the COM port to a router or Frame Relay Assembler/ Disassembler (FRAD), a gender adapter is required to convert the COM Port-to-Terminal/Printer cable's plug-type interface to a socket-type interface for the AUX port.

# Modular RJ45 (ISDN-U) Backup Interface

The backup connection is through the BKP interface/connector, which is an RJ45 8-position keyed modular jack. The following table shows pin assignments and the purpose of each.

The backup connection is through the BKP interface/connector, which is an RJ45 8-position keyed modular jack. The following table shows pin assignments and the purpose of each.

| Function | Circuit | Pin Number |
|---|---|---|
| Transmit/Receive ring to/from the local loop | R/R1 | 4 |
| Transmit/Receive tip to/from the local loop | T/T1 | 5 |




493-14342-01

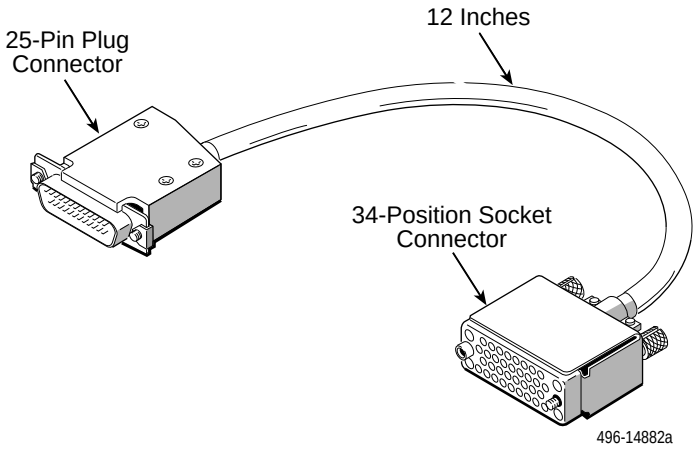
# EIA-232E Port 1 or 2 Interface

The following table shows the EIA-232E circuit and pin assignments that are supported for a port connector/interface (Port 1 or Port 2).

| Signal | Circuit Mnemonic | ITU/ CCITT # | Direction | 25-Pin EIA-232E Pin # |
|---|---|---|---|---|
| Shield | — | — | — | 1 |
| Transmitted Data (TXD) | BA | 103 | To DCE | 2 |
| Received Data (RXD) | BB | 104 | From DCE | 3 |
| Request to Send (RTS) | CA | 105 | To DCE | 4 |
| Clear to Send (CTS) | CB | 106 | From DCE | 5 |
| Data Set (or DCE) Ready (DSR) | CC | 107 | From DCE | 6 |
| Signal Ground/Common (SG) | AB | 102A | — | 7 |
| Received Line Signal Detector (RLSD or LSD) | CF | 109 | From DCE | 8 |
| Reserved for future use. | — | — | — | 9 |
| Not used. | — | — | — | 10 |
| Reserved for future use. | — | — | — | 11 |
| Reserved for future use. | — | — | — | 12 |
| Not used. | — | — | — | 13 |
| Reserved for future use. | — | — | — | 14 |
| Transmitter Signal Element Timing (TXC) | DB | 114 | From DCE | 15 |
| Reserved for future use. | — | — | — | 16 |
| Receiver Signal Element Timing (RXC) | DD | 115 | From DCE | 17 |
| Local Loopback (LL) | LL | 141 | To DCE | 18 |
| Not used. | — | — | — | 19 |
| Data Terminal (or DTE) Ready (DTR) | CD | 108/1, /2 | To DCE | 20 |
| Not used. | — | — | — | 21 |
| Ring Indicator (RI) | RI | 125 | From DCE | 22 |
| Not used. | — | — | — | 23 |
| Transmitter Signal Element Timing (TT) | DA | 113 | To DCE | 24 |
| Test Mode Indicator (TM) | TM | 142 | From DCE | 25 |

## V.35 DTE Adapter Cable (3100-F2-570)

Used as an interface between the 25-position Port 1 or Port 2 connector and a DTE's V.35 connector.



The following table provides the pin assignments for the 25-position Port 1 or Port 2 connector/interface and a DTE's V.35 connector.

| Signal | ITU/ CCITT # | 25-Pin Plug Pin # | Direction | 34-Pin Socket Pin # |
|---|---|---|---|---|
| Shield | — | 1 | — | A |
| Signal Ground/Common | 102 | 7 | — | B |
| Transmitted Data (TXD) | 103 | 2 (A)<br>14 (B) | To DCE | P (A)<br>S (B) |
| Received Data (RXD) | 104 | 3 (A)<br>16 (B) | From DCE | R (A)<br>T (B) |
| Request to Send (RTS) | 105 | 4 | To DCE | C |
| Clear to Send (CTS) | 106 | 5 | From DCE | D |
| Data Set Ready (DSR) | 107 | 6 | From DCE | E |
| Data Terminal Ready (DTR) | 108/1, /2 | 20 | To DCE | H |
| Data Channel Received Line Signal Detector (RLSD or LSD) | 109 | 8 | From DCE | F |
| Transmitter Signal Element Timing (TT) — DTE Source | 113 | 11 (A)<br>24 (B) | To DCE | U (A)<br>W (B) |
| Transmitter Signal Element Timing (TXC) — DCE Source | 114 | 15 (A)<br>12 (B) | From DCE | Y (A)<br>AA (B) |
| Receiver Signal Element Timing (RXC) — DCE Source | 115 | 17 (A)<br>9 (B) | From DCE | V (A)<br>X (B) |
| Local Loopback (LL) | 141 | 18 | To DCE | L |
| Test Mode Indicator (TM) | 142 | 25 | From DCE | NN |

# Technical Specifications

# F

| Specification | Criteria |
|---|---|
| **Network Access Module (NAM)** | |
| **Approvals** | |
| FCC Part 15 | Class A digital device |
| FCC Part 68 | Refer to the equipment's label for the Registration Number. |
| Industry Canada | Refer to the equipment's label for the Certification Number. |
| UL | Refer to the equipment's label for the UL listing. |
| CSA – Safety | Refer to the equipment's label for CSA safety information. |
| **Power Consumption and Dissipation** | 8.7 watts, 0.124 amps rms input current at 120 volts (ac power)<br>Result: 30 Btu per hour |
| **Weight** | 2.59 lbs. (1.18 kg) |
| **Physical Environment** | |
| Operating temperature | 35°F to 122°F (1.7°C to 50°C) |
| Storage temperature | 4°F to 158°F (20°C to 70°C) |
| Relative humidity | Up to 90% (noncondensing) |
| Shock and vibration | Withstands normal shipping and handling |

| Specification | Criteria |
|---|---|
| **Assembled 1-Slot FrameSaver Access Unit** | |
| **Power Consumption and Dissipation** | |
| 120 Vac power supply: | |
| Built-in power cord | NEMA 5-15P plug |
| Power consumption | 120 Vac, 60 Hz, 153 mA<br>Average power 9.5 W |
| Normal service voltage ranges | 120 Vac ±12 Vac, 60 Hz ± 3 |
| 80 – 220 Vac universal power supply: | |
| Built-in power cord | NEMA 5-15P plug |
| Power consumption | 100 Vac ~ 240 Vac ~, 0.7A, 50/60 Hz |
| Normal service voltage ranges | 100 – 240 Vac ±12 Vac, 2.5A, 12 Vdc, 50/60 Hz |
| **COM Port/Interface** – Communications/Management | 8-position modular unkeyed jack |
| Data rates | 9.6, 14.4, 19.2, 28.8, and 38.4 kbps |
| **Ports 1 and 2** – DTE Synchronous Data Ports | 25-position (DB25) subminiature connectors |
| Standards | EIA 232E, V.24, V.35 |
| Data rates | 4.8, 9.6, 14.4, 16.8, 19.2, 24, 28.8, 38.4, 48, 56, 64, 128, 192, and 256 kbps |
| **DDS Network (NET) Interface** | 8-position modular keyed USOC jack |
| Data rates | 56 kbps and 64 kbps clear channel |
| Services supported | 4-wire service, frame relay service, LADs |
| Physical interface (USA) | RJ48S |
| Physical interface (Canada) | CA48S |
| **Backup (BKP) Interface** – ISDN BRI DBM Backup | 8-position modular keyed jack |
| Physical interface | RJ49C |
| Service supported | ISDN service, 1B+D |

| Specification | Criteria |
|---|---|
| **Optional Features – ISDN BRI DBM** | |
| **Weight** | 0.27 lbs. (0.12 kg)<br>4.3 oz. (122 grams) |
| **Standards Compliance** | ANSI T1.601 – 1992 (physical layer)<br>AT&T Document 235-900-311, Issue 1.01 – March 1989<br>Bellcore SR-NWT-001937, Issue 1 – February 1991<br>Bellcore SR-NWT-002397, Issue 1 – June 1993<br>ITU Q.921 – 1992 (link layer)<br>ITU Q.931 – 1993 (network layer)<br>Northern Telecom NIS-S208-4 – October 1988<br>TR-TSY-00860, ISDN Calling Number Identification Services – February 1989, and Supplement – June 1990 |
| **Switch Compatibility** | National ISDN-1 (NI-1) |
| **Switched Network Interface** | One USOC RJ45 8-pole keyed modular plug and jack, specified in ISO/IEC 8877 |
| **Transmit Interface** | |
| Signal Level | 13.5 dBm nominal over frequency band, 0 Hz – 80 kHz |
| Impedance | 135 Ω |
| **Receive Interface** | |
| Dynamic Range | Operates on 2-wire loops, defined in ANSI T1.601-1992 |
| Impedance | 135 Ω |
| **Modulation and Frequency** | 2B1Q line coding with 4-level amplitude modulation (PAM) at 80K baud |
| **Channel Equalization** | |
| Receiver | Automatic adaptive equalizer with echo cancellation |
| **Power Consumption** | 60 mA at 15 Vdc<br>Average power .9W |

# Equipment List

# G

| Description | Model/Feature Number |
|---|---|
| **FrameSaver Access Units** | |
| FrameSaver Access Unit with ISDN BRI DBM (Includes 1-Slot Housing, 120 Vac Power Supply, COM Port-to-PC Cable, Network Cable, ISDN Cable, V.35 DTE Adapter, and Documentation) | 9620-A2-202 |
| FrameSaver Access Unit without ISDN BRI DBM (Includes 1-Slot Housing, 120 Vac Power Supply, COM Port-to-PC Cable, Network Cable, ISDN Cable, V.35 DTE Adapter, and Documentation) | 9620-A2-203 |
| FrameSaver Access Unit with ISDN BRI DBM, with Universal 80 – 220 Vac Power Supply (Includes 1-Slot Housing, COM Port-to-PC Cable, Network Cable, ISDN Cable, V.35 DTE Adapter, and Documentation) | 9620-A2-442 |
| FrameSaver Access Unit without ISDN BRI DBM, with Universal 80 – 220 Vac Power Supply (Includes 1-Slot Housing, COM Port-to-PC Cable, Network Cable, ISDN Cable, V.35 DTE Adapter, and Documentation) | 9620-A2-443 |
| FrameSaver Network Access Module (NAM) | 9621-B2-412 |
| FrameSaver Access Unit R1-to-R2 Upgrade (Includes Software Diskettes, Upgrade Instructions, and current Documentation) | 9620-C2-412 |
| **Optional Features** | |
| ISDN BRI Dial Backup Module (DBM) | 9098-F1-870 |
| Wall Mounting Kit for 1-Slot Housing | 9001-F1-891 |
| **User Documentation/Manuals** | |
| FrameSaver 9620 Access Unit Technical Reference (Paper Manual) | 9000-M1-004 |

| Description | Model/Feature Number |
|---|---|
| **Power Supplies** | |
| 120 Vac for 1-Slot Housing | 9001-F1-020 |
| 220 Vac for 1-Slot Housing (Universal Power Supply) | 9001-F1-040 |
| **Cables** | |
| V.35 DTE Adapter Cable<br>(connects Port 1 or 2 to DTE's V.35 interface),<br>EIA 530A-to-V.35 – 1′ | 3100-F1-570 |
| RJ45 Backup (BKP) ISDN-U – 20′ | 3100-F2-500 |
| COM Port-to-Terminal/Printer Cable,<br>8-pin modular-to-DB25P – 14′ | 3100-F2-540 |
| COM Port-to-PC Cable,<br>8-pin modular-to-DB25P – 14′ | 3100-F2-550 |
| COM Port-to-LAN Cable,<br>8-pin modular-to-DB25P – 14′ | 3100-F2-910 |
| RJ48S Network (NET) – 14′ | 3600-F3-501 |

# Glossary

| | |
|---|---|
| **agent** | A software program housed within a device to provide SNMP functionality. Each SNMP agent stores management information and responds to the manager's request for this information. |
| **aggregate** | A single bit stream that combines two or more bit streams. |
| **alternate destination** | A designated port, DLCI, and EDLCI that provides an alternate path for backup when the primary link or path is out of service. |
| **ASCII** | American Standard Code for Information Interchange. A 7-bit code that establishes compatibility between data services. ASCII is the standard for data transmission over telephone lines. The ASCII code consists of 32 control characters (nondisplayed) and 96 displayed characters. |
| **ASCII terminal/printer** | Devices that can be attached, either locally or remotely, to display or print the access unit's alarm messages. |
| **async terminal or emulation** | This feature allows a device to be controlled from an async (asynchronous) terminal like an ASCII (VT100-compatible) terminal. |
| **asynchronous** | A data transmission that is synchronized by a transmission start bit at the beginning of a character (five to eight bits) and one or more stop bits at the end. |
| **AT Command Set** | Attention Command Set. A group of commands, issued from an asynchronous DTE, that allows control of the modem while in Command mode. All commands must begin with the characters AT and end with a carriage return. |
| **ATM** | Asynchronous Transfer Mode. Cell-switching rather than frame relay technology. |
| **authentication-Failure trap** | An SNMP trap that indicates that the device has received an SNMP protocol message that has not been properly authenticated. |
| **Autobaud mode** | Access unit forces automatic redetermination of the DDS line rate/speed (56 or 64 kbps) as soon as a valid DDS network signal is detected. |
| **AWG** | American Wire Gauge. An indication of wire size. |
| **B channel** | ISDN Bearer Channel. A 56 or 64 Kbps channel that carries customer information like voice calls, circuit- or packet- switched data. Used for circuit-switched information by FrameSaver access units. |
| **BECN** | Backward Explicit Congestion Notification. A bit set and forwarded by the network to notify users of data traffic congestion, sent in the opposite direction of the frame carrying the BECN indicator or bit. Outbound frames may encounter congestion and be dropped. |
| **BKP** | Faceplate LED and rear panel label for the access unit's Backup interface. |
| **BPV** | Bipolar Violation. A modified bipolar signaling method in which a control code is inserted into the original data format. |
| **BRI** | Basic Rate Interface. An ISDN service rate of 144 Kbps, provided as two B-channels of 64 Kbps for information transfer and one D-channel of 16 Kbps for control and signaling. |
| **CC** | Cluster Controller. A device that handles remote communications for multiple async (or other VT100-compatible) terminals or workstations. |
| **CCA** | Circuit Card Assembly. A printed circuit board to which separate components are attached. |

**CCITT** Consultative Committee on International Telegraphy and Telephony, currently known as the International Telecommunication Union (ITU). See ITU.

**CD** Carrier Detect. A signal indicating that energy exists on the transmission circuit. Associated with Pin 8 on an EIA-232 interface.

**channel** An independent data path.

**CIR** Committed Information Rate. Less than or equal to the access rate, the CIR is used by the service provider for rate enforcement when the network is congested. When rates exceed the CIR, frames may be discarded. The management path has a CIR from 0 kbps to 64 kbps.

**circuit multiplexing** A proprietary method that provides the ability to multiplex the data of multiple DLCIs or data coming from multiple frame relay devices onto a single DLCI, sharing a single PVC connection.

**CNIS** Calling Number Identification Service. A service package ordered from the service provider that supports ISDN Caller ID.

**COM port** Communications port. A computer's serial communications port used to transmit to and receive data from a DCE. The DCE connects directly to this port.

**compression** With an access unit equipped with the data compression feature, serial data coming in from the DTE over Port 1 is compressed at ratios up to 4:1, encapsulated into a standards-based compression-transport protocol, then transmitted over the DDS network to frame relay PVCs. Also called data compression or synchronous data compression.

**configuration option** Device software that sets specific operating parameters for the access unit. Sometimes referred to as straps.

**configuration shortcuts** A feature that simplifies basic setup (configuration) of the access unit. Based upon the application selected, the access unit automatically configures certain options like DLCIs from information obtained from the network.

**CPE** Customer Premises Equipment. Terminal equipment supplied by either the customer or some other supplier, which is connected to the telecommunications network.

**CRC** Cyclic Redundancy Check. An error-detection technique used to confirm the integrity of received digital data. A series of two 8-bit block-check characters representing an entire block of data are generated and incorporated into a transmission frame, then checked at the receiving end.

**CSA** Canadian Standards Association.

**CSU** Channel Service Unit. The function of the access unit that protects the T1 line from damage and regenerates the T1 signal.

**CTS** Clear to Send. An EIA-lead standard for V.24 circuit CB, ITU 106; an output signal (DCE-to-DTE).

**data compression** The elimination of empty fields, redundancies, and gaps in order to reduce storage capacity needs and the amount of data to be transmitted. Anything that is compressed is restored after the data is received.

**DBM** Dial Backup Module. The optional internal ISDN BRI feature that provides automatic dial backup and service restoration of failed digital circuits. Provides an ISDN U-interface.

**DCE** Data Communications Equipment. The equipment that provides the functions required to establish, maintain, and end a connection. It also provides the signal conversion required for communication between the DTE and the network.

**D channel** A 16 Kbps ISDN channel that carries signaling information to control call setup, which may carry packetized information, as well.

**DDS** Digital Data Service, such as DATAPHONE Digital Service or ACCUNET Spectrum of Digital Services, that provides digital communication circuits.

**DE** Discard Eligibility. Part of the frame header that marks a frame for low priority if there is congestion on the network. If congestion occurs, DE frames are the first to be discarded by the network.

**decompression** With a unit equipped with the data compression feature, compressed data coming from the network is routed, de-compressed, then re-serialized for the DTE port.

**DLCI** Data Link Connection Identifier. The virtual circuit number corresponding to a particular connection between two destinations. This number is used as part of the frame relay header. The DLCI is always between devices, not just between endpoint devices. The total number of DLCIs between endpoints make up the PVC. DLCIs are a local means of identifying a PVC.

**DOC** Canadian Department of Communication.

**DSR** Data Set (or DCE) Ready. An EIA-lead standard for V.24 circuit CC, ITU 107; an output signal (DCE-to-DTE).

**DSU** Data Service Unit. Data communications equipment that provides an interface between the DTE and the digital network.

**DTE** Data Terminal Equipment. The equipment, such as computers and printers, that provides or creates data.

**DTR** Data Terminal Ready. An EIA-lead standard for V.24 circuit CD, ITU 108; an input signal (DTE-to-DCE).

**EDLCI** Embedded Data Link Connection Identifier. Use when multiplexing user data on a single DLCI (comparable to having multiple DLCIs on an interface being routed to a single DLCI on the network side). EDLCIs use a proprietary method to multiplex DLCIs that have been selected as one end of a connection. An EDLCI is a number between 0 and 62, and it identifies the individual connection within a multiplexed DLCI.

**EIA** Electronic Industries Association. This organization provides standards for the data communications industry to ensure uniformity of interface between DTEs and DCEs.

**encapsulated** Protocol-created control information that is added to the data or frame which has been broken into blocks or packets. The DTE constructs control packets and encapsulates user data within those packets.

**Enterprise MIB** MIB objects unique to a company.

**ESD** Electrostatic Discharge. An undesirable discharge of static electricity that can damage equipment and degrade electrical circuitry.

**excessive BPV** An excessive bipolar violation condition results when at least one invalid bipolar violation has occurred every 20 milliseconds for 2 seconds. A Health and Status message (under the Status branch/menu) is generated when this condition is detected.

**FCC** Federal Communications Commission. Board of Commissioners that regulates all U.S. interstate, intrastate, and foreign electrical communication systems that originate from the United States.

**FECN** Forward Explicit Congestion Notification. A bit set and forwarded by the network to notify users of data traffic congestion, sent in the same direction of the frame carrying the BECN indicator or bit. Inbound frames may encounter congestion and be dropped.

**FEP** Front-End Processor. A communications computer associated with a host computer that manages the lines and routing of data through the network.

**FRAD** Frame Relay Assembler/Disassembler. The equivalent of an X.25 PAD, a FRAD connects non-frame relay devices to the frame relay network. It also provides encapsulation and translation capability.

**frame** One identifiable group of bits that includes a sequence of bits for control, framing, etc.

**frame relay** A switching interface that is designed to get frames from one part of the network to another as quickly as possible.

**frame relay header** The DLCI identifier contained within the frame relay packet.

**frame relay switching** The ability to route frame relay packets based on the source port and frame relay header (DLCI). The header contains a DLCI identifier that distinguishes the port for which the data is intended.

**FRAW** Frame Relay Aware. Means the access unit can read the frame relay header and route the data internally to the correct port. This function allows an access unit using RFC1490 to distinguish its address on an incoming IP packet, and determine that the packet is for the access unit.

**FR Discovery** Frame Relay Discovery. A configuration shortcut method for automatic PVC configuration within the FrameSaver access unit. When the network interface is configured for the user side of LMI and this feature is selected, the unit creates a port DLCI for each DLCI coming from the network, and connects the two DLCIs.

**HDLC** High-Level Data Link Control. A communications protocol defined by the International Standards Organization (ISO).

**interface** A shared boundary between functional units.

**IP** Internet Protocol. The TCP/IP standard protocol that defines the IP as a unit of information passed across an Internet and provides the basis for packet delivery service. IP includes the ICMP control and error message protocol as an integral part. The entire protocol suite is often referred to as TCP/IP because TCP and IP are the two most fundamental protocols.

**ISDN** Integrated Services Digital Network. Telecommunication service that uses digital transmission and switching technology to provide voice and digital data communications on a bearer (B) channel while sending signaling on the data (D) channel.

**ITU** International Telecommunication Union. Formerly known as the Consultive Committee on International Telegraphy and Telephony (CCITT). An advisory committee established by the United Nations to recommend communications standards and policies.

**LAN** Local Access Network. A network designed to connect devices over short distances, like within a building.

**latching loopback** A loopback that can only be initiated or terminated by the 64 kbps clear channel network service provider.

**latency** Time it takes to transfer data from its source to its destination.

**LED** Light Emitting Diode. A light or status indicator that glows in response to the presence of a certain condition (e.g., ALM on the front panel for an alarm condition).

**LL** Local Loopback. An EIA-lead standard for V.24 circuit LL, ITU 141; an input signal (DTE-to-DCE).

**LMI** Local Management Interface. The standard set of procedures and messages that manage PVCs – the route between two DTEs. It is a common standard for link-management signaling (information exchange).

**loopback** Used to test various portions of a data link in order to isolate an equipment or data line problem. A diagnostic procedure that sends a test message back to its origination point.

| | |
|---|---|
| **LSD** | Line Signal Detect. An EIA-lead standard for V.24 circuit CF, ITU 109; an output signal (DCE-to-DTE). |
| **mesh network** | A network configuration where each node has a path to every other node. |
| **MIB** | Management Information Base. The set of variables a gateway running SNMP maintains. Standard, minimal MIBs have been defined, and vendors often have private enterprise MIBs. In theory, any SNMP manager can talk to any SNMP agent with a properly defined MIB. MIB-II refers to an extended management database that contains variables not shared by SNMP. |
| **multi-homed host** | A computer connected to more than one physical data link. The data links may or may not be connected to the same network. This function references the SNMP management function used by access units with multiple interfaces and potentially multiple IP node addresses. All access units will know about other access units that share PVCs and/or DLCIs through a form of RIP. The access unit directs traffic based on DLCI and EDLCI (switching), not through network protocol addresses (FRAD/router functions). The access unit only reads the frame relay header, not the data portion of the frame relay packet. |
| **multiplexing** | A method for interleaving several access channels onto a single circuit for transmission over the network. |
| **NAM** | Network Access Module. It is a type of CCA that accesses or interfaces with the network. |
| **NMS** | Network Management System. A computer system used for monitoring and controlling network devices. |
| **non-latching loopback** | A non-latching loopback can only be initiated or terminated by the 56 kbps network service provider. |
| **OOF** | Out Of Frame. An error condition in which frame synchronization bits are in error. |
| **OOS** | Out of Service. A digital network trouble signal. |
| **packet** | A group of control (header) and data characters (data and control signals) that are switched as a group within a communications network. |
| **PAD** | Packet Assembly and Disassembly. The term PAD is used extensively in X.25 networks; however, it can apply to any packet-switched network, such as frame relay. |
| **port aggregation** | Allows two ports to share a single frame relay link. |
| **PPP** | Point-to-Point Protocol. A link-layer protocol used by IP. |
| **primary destination** | A designated port, DLCI, and EDLCI for the primary data path from the data source so a PVC connection can be established. |
| **protocol** | The rules for timing, format, error control, and flow control during data transmission. |
| **PSTN** | Public Switched Telephone Network. A network shared among many users who can use telephones to establish connections between two points. |
| **PVC** | Permanent Virtual Circuit. This is the DSU's in-band management channel that supports remote management via a Telnet connection. It is the logical link, identified by a DLCI, used for routing frames over the network from their source to their destination. |
| **receiver** | A circuit that accepts data signals from a transmitter. |
| **RFC 1490 compliant** | The standard of multiprotocol interconnect over frame relay. This is the encapsulation method for carrying network interconnect traffic over a frame relay backbone; it also covers both bridging and routing. |
| **RIP** | Routing Information Protocol. Specifies the routing protocol used between access units. |

| | |
|---|---|
| **router** | A device that makes decisions about the paths network traffic should take and forwards that traffic to its destination. A router helps achieve interoperability and connectivity between different vendor's equipment, regardless of protocols used. |
| **RTS** | Request to Send. An EIA-lead standard for V.24 circuit CA, ITU 105; an input signal (DTE-to-DCE). |
| **RXC** | Received Clock. An EIA-lead standard for V.24 circuit DD, ITU 115; an output signal (DCE-to-DTE). |
| **RXD** | Received Data. An EIA-lead standard for V.24 circuit BB, ITU 104; an output signal (DCE-to-DTE). |
| **SDC** | Synchronous Data Compression. See compression. |
| **SDLC** | Synchronous Data Link Control. This is an IBM link-layer protocol. |
| **short packet** | Packet containing fewer than 80 bytes of data. |
| **SLIP** | Serial Line Internet Protocol. A link layer protocol used by IP. |
| **SNMP** | Simple Network Management Protocol. A generic network management system that allows the device to be managed by any industry-standard SNMP manager. |
| **status enquiry** | Message sent by the customer's frame relay equipment to maintain its user-network keep alive process, and requesting a status from the network. Network responds to each status enquiry frame. |
| **synchronous** | Data with an accompanying time signal. |
| **Telnet** | Virtual terminal protocol in the Internet suite of protocols. Allows the user of one host computer to log into a remote host computer, and to interact as a normal terminal user for that host. |
| **throughput** | Amount of data, or the number of data units per units of time, that pass through the network when it is operating a peak capacity. |
| **TM** | Test Mode. An EIA-lead standard for V.24 circuit TM, ITU 142; an output signal (DCE-to-DTE). |
| **transmitter** | A circuit capable of generating, modulating, and sending a signal for communication, control, and other purposes. |
| **TXC** | Transmit Clock. An EIA-lead standard for V.24 circuit DB, ITU 114; an output signal (DCE-to-DTE). |
| **TXD** | Transmit Data. An EIA-lead standard for V.24 circuit BA, ITU 103; an input signal (DTE-to-DCE). |
| **UL** | Underwriter's Laboratories, Inc. An organization which promotes product safety. |
| **UNI** | User-to-Network Interface. This is the frame relay interface, located between the unit and the network. |
| **USOC** | Universal Service Ordering Codes. Generic telephone company service ordering codes. |
| **Vac** | Volts alternating current. |
| **virtual circuit** | A logical link/connection or packet-switching mechanism established between two devices at the start of transmission. |
| **WAN** | Wide Area Network. A network that spans a large geographic area (e.g., a country). |

# Index

## Numbers



## A

## B



## C

## D

## E

## F



## G



## H



## I

# L

## M



## N

## O



## P

## Q



## R



## S

## T

## U

## V



## W